

SWEET BRIAR COLLEGE



3 2449 0472434 2



Digitized by the Internet Archive  
in 2010 with funding from  
Lyrasis Members and Sloan Foundation

<http://www.archive.org/details/hackedtobitshack00baxl>

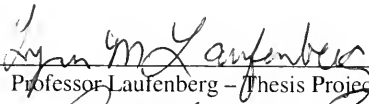


# Hacked to Bits

Hacking and Cyberpolicy in the 21<sup>st</sup> Century

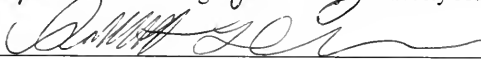
Senior Honors Thesis  
in the departments of  
Computer Science and History  
By Caroline Baxley

Defended and Approved March 31, 2006



Professor Laufenberg – Thesis Project Faculty Advisor – date

5/2/06



Professor Chase - date

5/3/2006

Dr. Svoboda – date



From:

05/03/2006 10:42 #009 P.002/002

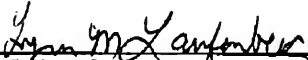
48 6F 6E 72 27 73 20 54 68 65 73 69 73

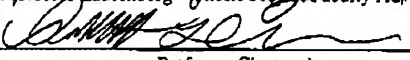
# Hacked to Bits

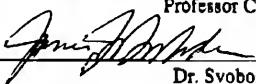
Hacking and Cyberpolicy in the 21<sup>st</sup> Century

Senior Honors Thesis  
in the departments of  
Computer Science and History  
By Caroline Baxley

Defended and Approved March 31, 2006

 5/2/06  
Professor Lautenberg - Thesis Project Faculty Advisor - date

 5/3/2006  
Professor Chase - date

 5/3/2006  
Dr. Svoboda - date



## Abstract

*This paper will look at the current state of “hacking” – how we define the act of hacking both in the mainstream media and in the law and what sorts of “things” hackers do. It will discuss the differences between legal and illegal hacking, illustrating examples of both and explaining the distinctions between the two. It will also look at some of the effects the rise in illegal hacking has had on people who have become more privacy obsessed and interested in their digital rights and preserving their individual identity. This paper will then look at two different approaches to solving the problems created by hackers – the defenses put in place by network security and the legislation designed by government (specifically US). It will compare the two methods and discuss the results of the combined approaches.*

## Table of Contents

<b>Section 1 – Introduction.....</b>	<b>3</b>
<b>Section 2 – What are Hackers.....</b>	<b>9</b>
<b>Section 2.1 – Definitions.....</b>	<b>9</b>
<b>Section 2.2 – The Current State of Hacking.....</b>	<b>12</b>
<b>Section 2.3 – Illegal Hacking.....</b>	<b>14</b>
<b>Section 2.4 – Recent Cybercrime Cases.....</b>	<b>15</b>
<b>Section 2.5 – Computer Crime and Privacy.....</b>	<b>18</b>
<b>Section 2.6 – Information Privacy.....</b>	<b>21</b>
<b>Section 2.7 – Identity Theft.....</b>	<b>24</b>
<b>Section 2.8 – Legal Hacking.....</b>	<b>27</b>
<b>Section 2.9 – Summary / Conclusion.....</b>	<b>29</b>
<b>Section 3 – Who are Hackers.....</b>	<b>30</b>
<b>Section 3.1 – Types of Hackers.....</b>	<b>30</b>
<b>Section 3.2 – Script Kiddies.....</b>	<b>33</b>
<b>Section 3.3 – Black-Hat Hacking.....</b>	<b>36</b>
<b>Section 3.4 – Bad Code: Viruses, Worms and other malware.....</b>	<b>38</b>
<b>Section 3.5 – Helpful Hackers (white hat), Security Specialists.....</b>	<b>40</b>



<b>Section 3.6 – Hacker forums.....</b>	<b>42</b>
<b>Section 3.7 – Summary / Conclusion.....</b>	<b>43</b>
<b>Section 4 – What do we do about Hackers.....</b>	<b>45</b>
<b>Section 4.1 – Vulnerable Machines.....</b>	<b>45</b>
<b>Section 4.2 – Copyright Protection.....</b>	<b>47</b>
<b>Section 4.3 – P2P and other filesharing networks.....</b>	<b>50</b>
<b>Section 4.4 – Privacy Protection in Policy.....</b>	<b>52</b>
<b>Section 4.5 – Network Security.....</b>	<b>53</b>
<b>Section 4.6 – Information Security.....</b>	<b>56</b>
<b>Section 4.7 – Upcoming Changes.....</b>	<b>59</b>
<b>Section 4.8 – Combining Approaches.....</b>	<b>61</b>
<b>Section 4.9 – Summary / Conclusion.....</b>	<b>63</b>
<b>Section 5 – Conclusion.....</b>	<b>65</b>



## Introduction

A hacker, curious about a network's defenses, noses around until he finds a way to break in. He then leaves a message for the network administrator, telling him where the system is weak. He may leave his name but he does little damage and is gone as quickly as he came. Without his helpful advice, the network administrator may not have even known the hacker was there. Is this hacker good, bad, or somewhere in between?

That hacker would be Adrian Lamo, a "grayhat" hacker well known for his exploits in exploiting websites and then sending the fixes to network administrators. Excite@Home praised him for helping them find vulnerabilities which would allow attackers to access part of the corporate network through the webpage.<sup>1</sup> "Lamo is 'someone who tries to uncover security holes with good intentions--to show us where we had some security holes, so those could be fixed,' Corder, the spokesperson for Excite@Home, said.

Companies are rarely so accepting of the help of these helpful hackers. Lamo continued his exploits, hacking Yahoo! News, WorldCom, and Microsoft.<sup>2</sup> Then in 2002, Lamo hacked the website of *The New York Times*, putting his name on their list of accepted sources and using their Lexis-Nexis account to run searches. This was not taken so well as his previous escapades and after a five-day manhunt by the FBI, Lamo surrendered in Sacramento, CA.<sup>3</sup> His case only serves to highlight the confusing problem of hackers and their intentions. While Lamo was illegally accessing systems which contained very valuable information, he never deleted or harmed the system, only offering his help in fixing the problem he exploited before he took the

---

<sup>1</sup> Lemos, Robert. "Hacker helps Excite@Home toughen defenses." *CNet News*. May 29, 2001. Accessed 3/4/06. <<http://news.com.com/2100-1001-261728.html>>

<sup>2</sup> <http://www.securityfocus.com/news/254>, <http://www.securityfocus.com/news/296>

<sup>3</sup> [http://news.com.com/Homeless+hacker+surrenders/2100-1009\\_3-5073426.html?tag=nl](http://news.com.com/Homeless+hacker+surrenders/2100-1009_3-5073426.html?tag=nl)



security flaw public. He always claimed his intentions were good, but many companies resented his intrusion, though they used his information to fix their systems.

Hackers - once only known among computer-geeks in the dawn of the computer age as the most clever and innovative of programmers, have now taken on a more sinister role as the media popularizes them as burglars and thieves. When thinking about hackers, a specific image often comes to mind, an image shrouded in mystery as the hacker commits his crimes under an alias, until he emerges as a young man following the police in handcuffs into the eyes of the world's cameras. But to the people whose job it is to protect networks, the hacker's motives are irrelevant. The network administrator wants to keep the hackers out, to patch all the holes in his system, to try to outwit the hacker at every turn. While legislatures rush to define the new crimes that have emerged in the cyber age and law enforcement studies how to track hackers, the network administrators must learn how the hackers will attack in order to make their systems secure. It takes cooperation on all sides to defeat the hackers.

Today's hackers come in two forms. One is the "good" hacker, the "white-hat hacker," security specialist, legal hacker, and curious person experimenting with his own electronics to discover how they work and how to make them work better. These hackers work to increase the body of knowledge concerning computer security and hacker defense, much as their predecessors did in the early days of computing. They come up with inventive solutions to problems, clever ways to get around security, and they help security researchers discover the weaknesses in their systems so patches can be released. The other is the black-hat hacker, the "cracker," the malicious hacker out to destroy information or the criminal intent on fraud. Both groups spur innovation – the good by discovering new techniques to improve electronics by making them more efficient, more secure and more functional. The bad hackers spur innovation



by discovering security holes before they are patched and exploiting them, forcing programmers and designers to go back, fix their work and make it secure against future attacks of a similar nature.

Network security is an on-going war between net administrators struggling to keep the latest software installed on the latest hardware and hackers doing their best to exploit every possible weakness the net administrators have missed. Network security protects information, whether that information is a user's homework and website, or more sensitive information, such as their bank accounts, their credit card information, or their transcripts. Some people specialize in protecting this information; others specialize in gaining access to it. This information is the commodity hackers are interested in gaining; social security numbers, breaking the copyright protection on the latest DVD, medical records, new music, a foreign nation's weapons development. It falls to network security specialists to do just that.

However, it is the malicious hackers that network security works so hard to stop. Firewalls, spyware and virus scans, encryption and various other protections are all designed to prevent hackers from accessing information they should not be allowed to see. Information, whether in the form of a bank statement, a homework assignment, an email or picture, is a commodity people want protected. They are willing to pay experts to protect their systems from hackers who would try to steal or destroy the information those systems contain.

The government makes an effort to protect our online rights. Anti-spam<sup>4</sup> and computer fraud<sup>5</sup> policies have followed in the wake of major computer crimes in an attempt by the government to regulate some of the felonies that have become more common with the prevalence of the Internet. Government regulation provides the backbone of Internet policy; it regulates the

---

<sup>4</sup> CAN-SPAM Act of 2003. Enacted Jan 1, 2004, Pub. L. 108-187, S. 877

<sup>5</sup> PROTECT Act, USA PATRIOT Act and others <<http://www.cybercrime.gov/cclaws.html>>



code which controls the Internet<sup>6</sup>. But while government policy can dictate the law, network security has the responsibility of enforcing the actual protection of this privacy. A secure network is the first line of defense against hackers. And with government creating laws to back security policies, illegal hacking can then be prosecuted.

While many people have looked at hacking from a legal perspective, others focus on it solely from a defensive standpoint in network security. This paper aims to bring these two standpoints together, looking at hacking as it is seen and defined from both these views and discussing how each chooses to combat and discourage it. This paper will also discuss what occurs where government restrictions end and the choice of a more secure or free network is left to the administrator and the user, who can choose how much protection or freedom they are granted.

This paper will address hacking in three parts. First, it will look at the current state of “hacking” – how we define the act of hacking both in the mainstream media and in the law. It will discuss the differences between legal and illegal hacking, providing examples of both and explaining the distinctions between the two. It will also look at some of the effects of the rise in illegal hacking. This section will also discuss identity theft and privacy issues one faces when dealing with hackers and introduce some of the most recently prosecuted cases of computer intrusion to illustrate the most current jurisprudence. The focus of this section is to define who hackers are and what exactly it is they do. This section will also look at current cases involving hackers to see what the trends are and how the legislation is dealing with the problem.

The second part will focus on hackers themselves. They range from the ragged teenagers to skilled computer users with a mission. What motivates them to hack? How do hackers manage

---

<sup>6</sup> Lessig, Lawrence. *Code and other Laws of Cyberspace*. Basic Books, New York; 1999. Lessig argues that the Internet is not inherently free as many would assume, but is regulated by code and if government wants to regulate the Internet, it must start by regulating the code that creates it.



to get around all the different sorts of protections that we diligently put on our computers? This section further explores topics addressed in the first section, bringing up the important question of who hackers truly are. The main difficulty in presenting a clear picture is that this group defies easy explanation, some fitting in categories neatly while others are surprising.

In the third section the paper will look at various methods of hacker prevention through good network security practices and legislation designed to discourage certain activities. While no single method can guarantee complete security, some methods are far more effective at deterring hackers and keeping out all but the most skilled and determined. Prevention of illegal hacking and protection of privacy is the responsibility of each person who uses computers. It is accomplished through awareness of hackers and their methods and by implementing good security practices. Security specialists learn about new hacker methods in order to defend their networks, individual users put up firewalls and run anti-spyware programs in an attempt to block and remove holes in their systems. No one method guarantees protection, but taken together, they can provide practical security for most computer users.

The problem of hackers, or people who can circumvent network security measures, is important because it highlights both the inherent insecurities of any open information-exchange system (hackers were known to go after phone systems long before computers existed) as well as a threat to individual privacy (due to our growing reliance on the Internet). While it may be difficult to exactly identify hackers or their methods of attack, studying and understanding the general stereotypes allows security to develop strong defenses against all but the most determined of hackers. Studying both hacker methods as well as various common preventions and the laws concerning hackers highlights the various problems and solutions as well as the holes that are more difficult to fill.



So, who are the hackers? What do they do? How do network security and government approach the problem of defining the crimes and creating deterrence for those who would participate? What is the result of these restrictions when taken together? And, can we ever truly define hacking or is the problem far more complicated than it seems? This paper will try to explore all these questions, to look at who we think hackers are and where they surprise us and what those surprises mean to people who are trying to prevent them. It will finally conclude that the people who make up the term hacker defy simple explanation. Sure, some can be easily categorized, but there is just as much of a threat from the unexpected. To deal with these hackers, both the expected and unexpected, network security must be vigilant and prepared and legislatures must try to make laws that are both inclusive of all possibilities but not so restrictive that they hurt the liberties of those who are not engaged in crime. There are no completely secure networks and so users must accept some level of risk when using a networked computer.



## Section 2 – What are Hackers?

### 2.1 – Definitions

Some technical computer terms that seem straightforward are actually complex, having different meanings depending on context. Terms relating to computers and the people who use them have changed as fast as the technology itself has grown and have become part of mainstream popular culture. The term hacker, for example, conveys the popular meaning of a malicious person who breaks into computers and steals information. However, within the programming community, hacker means something completely different. They first coined the term to mean someone who is a particularly clever programmer.

*Hackers*, however you choose to view them, are generally defined as people who are “gifted at extending the function of computers beyond their original design.”<sup>7</sup> What, exactly, they do with their expertise is where the definition becomes clouded. While originally a term referring to a clever computer programmer who came up with a new or particularly inventive way to solve a problem, the term has evolved (mainly due to negative use by the media) into its more common usage as a reference to a computer criminal.

The most common usage of "hacker" in the popular press is to describe those who subvert computer security without authorization or [...] anyone who has been accused of using technology (usually a computer or the Internet) for terrorism, vandalism, credit card fraud, identity theft, intellectual property theft, and many other forms of crime. This can mean taking control of a remote computer through a network, or software cracking. This is the pejorative sense of hacker, also called cracker or black-hat hacker or simply "criminal" in order to preserve unambiguity.<sup>8</sup>

This paper will discuss several different types of hackers, both the white- (legal) and black- (illegal) hat varieties. Unless specified, however, hacker will be used in the pejorative

---

<sup>7</sup> Skouis, Ed. *Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Prentice Hall PTR, Upper Saddle River, NJ; 2002.

<sup>8</sup> Wikipedia. <<http://en.wikipedia.org/wiki/Hacker>> July 25, 2005. Despite Wikipedia's changing nature, this definition does the best at capturing the most complete definition of hacking.



sense, as a computer criminal as this is the most common usage of the word at this time, though no offense is intended to those who consider themselves *rather good hacks* or hackers in the sense of “they are clever programmers.”

**Computer** is another term which, like hacker, has multiple meanings. It is more than a vague reference to a machine which can do electronic calculations. Many people see a personal desktop or laptop with a “Dell” or “Apple” logo on it and think that it is a computer. In this they are technically correct. But ‘computer’ covers a far wider range of machines than the personal boxes and laptops most people are familiar with.<sup>9</sup> Hidden away in frigid rooms are racks of powerful servers and routers that connect scores of personal units to each other and out to the wider world. These computers are far more specialized than the familiar desktop units. And over the Appalachian Mountains at Virginia Tech is a collection of Apple XServe G5 nodes rigged together to create a powerful supercomputer.<sup>10</sup> All these are types of computers that hackers want to compromise. Computer intrusion involves the unauthorized access of any one or more of these types of computer. A server can be just as much of a target as an individual’s laptop. It is important to recognize that the types of computers hackers target vary as much as do hackers’ intentions and goals. They access these computers not by physically breaking in the building where the computer is housed, but accessing it from a remote location, connecting to the target computer through a series of other computers.

Any time one computer connects to another, it creates a **network**. This system can be as simple as two computers hooking up to transfer files, five computers hooked to the same printer, a dozen computers sharing information from a server, or the countless computers around the

---

<sup>9</sup> Computer is defined as “A calculating-machine; esp. an automatic electronic device for performing mathematical or logical operations” Computer definition 2. *The Oxford English Dictionary*. Oxford University Press. Accessed 2.26.06

<sup>10</sup> <http://www.tcf.vt.edu/index.html>



world that connect to form the Internet. Networks facilitate sharing of information, of printers, of files, and of personal details. This act of sharing and the exchange of computer information that goes along with it is what hackers exploit in their efforts to gain admittance to protected computers. The interconnectivity of a network is a convenient pathway to legally and illegally access another's computer; the standardized file sharing protocols are vulnerable to easy access to another's computer or a prohibited area on a computer to which you are invited or granted access. However, "secure" data may be obtained other ways: reading others' trash, photographing monitor screens, criminally purchasing data or access codes from insiders, intercepting electronic radiation. Networks form an integral part of modern computers and have many positive uses, but they are also the primary means by which hackers access information.

There are several types of networks. LANs (Local Area Networks) generally connect computers within a contained geographic area, such as a building, or a school campus. WiFi (Wireless) networks, which are generally attached to a larger LAN, involve the use of one (or more) wireless routers to carry information through the air. VPNs (Virtual Private Networks) simulate a LAN connection across the Internet. Data security can come in many forms; network access security, individual computer access controls, encryption of data, physical separation of "secure" servers, wires, and connections, records disposal, vetting of employees, and compartmentalization of knowledge. Like each method of keeping data secure, each different type of network has its own strengths and weaknesses, which a hacker will know and exploit.

Hacker, computer, and network are the basic concepts this paper will use in exploring hacking, though there is much more detail in each area that can be examined. And these basic technologies change. What we consider a pocket calculator today was a massive computer years ago. And as we progress, computers will continue to become more powerful and likely even



more integrated into our everyday lives. This paper deals with computers and hacking in their current form, though even that changes frequently.

## **2.2 – The Current State of Hacking**

Computer intrusion can be thought of as a form of digital trespassing; the hacker gains unauthorized access to a protected computer, going onto someone else's property uninvited.<sup>11</sup> A computer in an Internet café, for example, often does not require any form of authentication to log into. Of course, valuable information should not be stored on an Internet café computer since one never knows who will be using it afterwards, though this does not stop some from accidentally using it to send credit card information to a site. This Internet café computer could still be accessed illegally. The owner authorizes the use of their computers for a specific time after you have paid (or agreed to pay) for the amount of time used. Without the owner's permission, the access of these computers is unauthorized.

The primary US federal laws concerning hackers, United States Code 18, Sections 1029 and 1030, "Fraud and Related Activity in Connection with Access Devices/Computers," clearly defines the term "access device" (anything used to illegally access a computer such as a password) and what kinds of illegal access leads to prosecution (data related to national security, financial data, medical records, unauthorized access of any government computer and any data with a value greater than \$5000).<sup>12</sup> This law also allows for the prosecution of any computer intrusion crime that causes damage, both reckless and intentional. The sentences contain

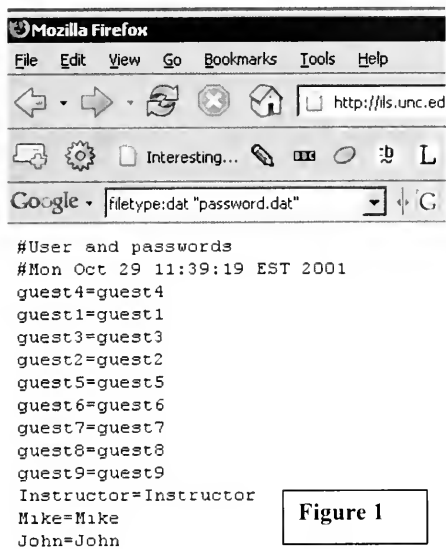
---

<sup>11</sup> Unauthorized access means the hacker is not supposed to be on that computer for any reason. A protected computer means a computer which authorization is required to access.

<sup>12</sup> "any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds" 18 U.S.C. 1029 (e)(1); 18 U.S.C. 1030.



punishments that include 5 to 20 years in prison, various fines, and the removal of any computer access.



**Figure 1**

and the Google Bots do an surprisingly efficient job indexing everything on the net. This means information can be easily found that can be used to exploit computer systems.<sup>13</sup> For example, a quick Google search for “allinurl:tsweb/default.htm” lead to a law firm’s remote desktop login. Another search string “intitle: ‘Index of’ config.php” brought up some password lists contained in the config.php files. And yet another Google search, “filetype:dat ‘password.dat,’” brought up a list of usernames and passwords.<sup>14</sup> (Figure 1). This is one of the straightforward examples as it features no encryption so the passwords (which are set to be the same as the username) are easy to read and require no further work to decipher. Others found in the same search featured encryption or foreign characters which would have to be broken before they revealed their

Computer fraud is easy to accomplish with a little technical knowledge. One simple and popular type of hacking is *Google Hacking*, which allows people with relatively little knowledge of hacking to find out an amazing amount of information. Since information can be found on a range of random computers, hackers using Google are generally looking for easy prey rather than a specific target. The Google search engine is a powerful tool for finding information

<sup>13</sup> McClure, Stuart. *Hacking Exposed: Network Security Secrets and Solutions – Fifth Edition*. McGraw-Hill, New York; 2005. pp 2.

<sup>14</sup> Google hack strings from <http://johnny.ihackstuff.com/index.php?module=prodreviews> Accessed August 14, 2005.



passwords. Google hacking is an easy place to start gathering information on systems which are vulnerable for break-ins. Whole websites such as Johnny.ihackstuff.com and The Hackers Choice at thc.org are dedicated to helping young hackers learn their way about the Internet and discover all about the information that can be found on the Internet for those who know where to look for it and are curious enough to explore.<sup>15</sup>

Hacking is an evolving art. Today, tools such as Google search are popular for hackers, but soon they will come up with new ways to exploit computers and their methods of attack will change. Whether one is just gathering information on security loopholes or looking for someone's bank information, the connectivity of the Internet provides the tools to make this process easier and sharing of information more mechanized.

### **2.3 – Illegal Hacking**

The type of hacking that gets the most media attention is illegal or criminal hacking. The constant use by the media of the term 'hacker' in a negative fashion is the reason the term is so commonly associated with computer criminals and why most people will give the pejorative definition of the word when asked. The actual act of hacking is generally only a small portion of the crime committed. The term 'hacker,' however, has grown to cover anyone who uses unauthorized access to electronic information to commit their crime. It is not the hacking so much as the damages caused after the hacking is successful that catches legal attention. While the hacking itself is illegal, it is generally not the only reason hackers are prosecuted. They are prosecuted for the damage they create, the information they access, or the security they weaken from their exploration. Computer crime cases contain counts of computer access fraud, as well as some further crime or violence committed in conjunction with that unauthorized access. These

---

<sup>15</sup> Thc.org or The Hackers Choice who advocate hacking so that you "don't get caught", give lists of their latest exploits and "a collection of several hacking tools." <http://www.thc.org/papers/COVER-1.TXT/>, <http://www.thc.org/exploits.php> and <http://www.thc.org/root/>. Accessed 9.16.05.



crimes are often fraud, such as credit card theft, or malicious destruction, such as intentionally crashing the system that has been hacked.

Several recent cybercrime cases, which are tried with growing frequency, highlight the current trends in criminal hacking. These are the cases that the media pays attention to and are used to define the changing scope of hacking crimes. They include instances of spam (sending lots of unwanted email), phishing (a scam which asks for personal information, generally a prelude to identity theft), fraud (the uses of illegally obtained data to facilitate fraud) and system destruction (service disruption).

## **2.4 – Recent Cybercrime Cases**

18 U.S.C 1030 was first drafted in October of 1984, though it was updated regularly after that until 2001.<sup>16</sup> It was drafted in response to a rise in computer crimes in the 1980s. The first case convicted under the Computer Fraud and Abuse act was Robert Morris, whose Internet worm crashed over 6,000 government and university computers. He was sentenced to three years probation and a \$10,000 fine. While the sorts of crimes have evolved since then and simply crashing a network has been replaced by phishing and spyware and zombie computers, the Computer Fraud and Abuse Act is still the primary legislation under which hacking is prosecuted.

On July 14, 2005, the Department of Justice, Eastern District in Pennsylvania convicted Allan Eric Carlson (age 42) of 79 counts of computer and identity fraud and sentenced him to four years in prison. He hacked into several computers and used them to send out massive amounts of spam. The “from” line of the email contained a valid email address belonging to another person. Since many of the addresses he sent his spam “to” were invalid, tons of bounced

---

<sup>16</sup> [http://pirate.shu.edu/~jenninju/InternetLaw/09\\_Cybercrime/COMPUTERFRAUDABUSEACT18USC1030.htm](http://pirate.shu.edu/~jenninju/InternetLaw/09_Cybercrime/COMPUTERFRAUDABUSEACT18USC1030.htm)  
Accessed 4.6.06.



On November 17, 2005, in Washington D.C., the six men responsible for the Shadowcrew.com website plead guilty to counts of identity theft and credit card fraud. Not only did they steal people's identities and credit information, they also aided known criminals in getting false identification. Mantovani, one of the operators, used "techniques such as phishing and spamming to illegally obtain credit and bank card information, which he then used to make purchases of merchandise online. The illegally obtained goods were then sent to a "drop" or mailing address specifically set up to receive the stolen goods."<sup>20</sup> The operation was busted by the Secret Service in 2004 and the six men face penalties of up to five years and \$250,000 for each count. This website was one well-organized network of identity thefts, out to steal the personal information of as many people as possible.

On January 23, 2006, in the first prosecution of its kind in the US, Jeanson James Ancheta plead guilty to creating and using bots to scan for vulnerable computers, infect them by placing itself on a computer, and use the computers to issue attacks of various forms against other computers. His armies of bots, which were sold to hackers to use in denial of service attacks (where a network is so saturated in false traffic that it cannot handle real traffic), took over unsuspecting computers. He was charged with accessing protected computers, including federal computers used for the nation's defense. He not only has to repay all the money he earned illegally, but faces a maximum sentence of 25 years.<sup>21</sup>

Each of these cases highlights the growing recurrence and changing themes in computer crimes. From selling programs that allow spying on individual computers to programs which take over armies of computers, these criminals are clever and resourceful in obtaining their goals

---

<sup>20</sup> "Six Defendants Plead Guilty in Internet Identity Theft and Credit Card Fraud Conspiracy" <<http://www.cybercrime.gov/mantovaniPlea.htm>> Accessed 1.29.06.

<sup>21</sup> "Bot Herder Pleads Guilty to Fraudulent Adware Installs and Selling Zombies to Hackers and Spammers" <<http://www.cybercrime.gov/anchetaPlea.htm>> Accessed 1.29.06.



and illegally earning money through promoting their product. They steal information from people, spam victims with unsolicited information, use their skills to hack and crash systems – none of which is legal. But all these criminals have been caught and are in the process of being sentenced as an example to others who might wish to duplicate their stunts. Each of these crimes involved hacking and each involved some measure of privacy invasion, the victim losing his email address, control over his computer, or his identity and credentials.

## **2.5 – Computer Crime and Privacy**

One of the major legal issues hackers face when being prosecuted for their computer crimes is their violation of a person or a company's privacy rights. "You have zero privacy anyways...get over it," said Scott McNeally, founder of Sun Microsystems.<sup>22</sup> This phrase highlights one end of the spectrum of ideas when it comes to computerized information and the privacy of that information. With the pervasiveness of digital information, and with the duplication of digital information being cheap and easy, the music and movie industries are not the only ones who are worried about hackers stealing their money and their work. Any time information is put on a machine which is connected to a network it becomes a privacy risk. Maybe a hacker will break into the company's database and steal project plans and blueprints.<sup>23</sup> Maybe a server's administrator enjoys reading the emails that pass through his server; and there is a good chance your computer has recently downloaded some sort of program that, until you remove it, reports your every move to a marketing company interested in what kinds of products

---

<sup>22</sup> Polly Sprenger, Sun on Privacy: "Get Over It", Wired News, Jan. 26, 1999, at <http://www.wired.com/news/politics/0,1283,17538,00.html>.

<sup>23</sup> Mitnick, Kevin. *The Art of Deception: Controlling the Human Element of Security*. Wiley Publishing, Inc., Indianapolis, Indiana; 2002.



you look at online.<sup>24</sup> Because information is so easy and cheap to share online, the amount of information that gets shared is increased and your privacy is reduced.

On the other side of the privacy discussion fall people who use anonymous re-mailers, encryption, or simply refuse to perform any transaction online.<sup>25</sup> They recognize that the system is far from secure and are convinced that they are going to become the next victim in the increasingly advertised problem of identity theft. They believe they have a right to privacy and go about diligently enforcing it. Services such as MuteMail, which advertises itself as a secure and anonymous email service, and Anonymizer, which offers anonymous Internet surfing and encryption services, help users gain security and protection for online transactions.<sup>26</sup> But their use of these services indicates their understanding of their own vulnerability. It indicates their vulnerability to the mechanisms of others who would desire to invade their privacy.

Then there are the people in the middle who are aware of the problem but do not let that deter them from completing their transactions online. This group includes the average Internet user. They are unwilling to give up their easy access to the net and their online transactions and just hope they do not become the next fraud victim. Or they assume that with so many people out there it is unlikely they will be targeted and that if they take the basic steps to keep them from being an easy target, they will be safe. These are the people most frequently targeted as they have plenty to lose but often inadequate protection. When a hacker sweeps a network looking for victims, the search is random and those attacked are those with the least protection, the systems easiest to break into.<sup>27</sup> These people believe they have a right to privacy, but are ineffective in

---

<sup>24</sup> Spyware can be defined as "Software to observe user behavior to collect information under users' noses." <[http://web.interhack.com/publications/spyware\\_intro.php](http://web.interhack.com/publications/spyware_intro.php)> Accessed 9.16.05.

<sup>25</sup> Simmons, Dan, "The cost of online anonymity." *BBC News Online*.

<[http://news.bbc.co.uk/1/hi/programmes/click\\_online/4227578.stm](http://news.bbc.co.uk/1/hi/programmes/click_online/4227578.stm)> posted 9.12.05 accessed 9.16.05.

<sup>26</sup> <http://www.mutemail.com/>; <http://www.anonymizer.com/>

<sup>27</sup> McClure pps 646.



their personal defenses of their privacy. Here is where the law steps in – determining exactly how much privacy a user has a right to expect.

Thinkgeek.com, the ultimate shopping site for geeks and gadget freaks, carries a bumper sticker that claims, “i read your email.”<sup>28</sup> But with hundreds of thousands of email messages flying around the Internet every day, who really has time to sit down and read through them all? Sure someone *could* be reading your emails, but would be highly unlikely. A similar idea applies to the encryption used for online transactions. Someone *could* break the encryption with enough time and resources, but it is likely to cost more to break the encryption than the data gained would be worth.<sup>29</sup> Thus the encryption is considered to be *practically* secure, secure for all practical purposes even though in theory it could be broken. Privacy practically exists, but can certainly be violated by a determined party.

So if we assume that someone *can* access any electronic information you may have, the question becomes a privacy issue – how much privacy can one expect to be assured by the government? The debate over privacy rights has been going on since long before anyone dreamed of electronic communication or the Internet. It is only heightened by the ease with which digital information can be accessed, both legally and illegally, and so suggests one issue of privacy, but also an issue of storage location.<sup>30</sup> Does the protected data have to be stored on a machine that is owned by the person whose information it contains in order to be considered protected data? Take a piece of information, say, a bank statement. As long as only one person knows that information, then it is private. But what if it is typed to a document and saved on a local hard drive? If the hard drive is connected to the Internet, a hacker could access that

---

<sup>28</sup> <<http://www.thinkgeek.com/cubegoodies/stickers/36e8/>> They also carried a t-shirt which says the same, but I was unable to find a link for it.

<sup>29</sup> Mel, H.X. *Cryptography Decrypted*. Addison-Wesley, Boston; 2001. pp 35.

<sup>30</sup> DeVries, Will Thomas. "Protecting Privacy in the Digital Age." *Berkeley Technology Law Journal*. 18 Berkeley Tech. L.J. 283. 2003.



information. If a hacker broke into the computer to get the information, it would be an invasion of privacy because the physical machine on which the information resided was compromised. But what if, instead of storing the document on a hard drive, it was stored using a net storage service located far away from any personal computer – would accessing it there be an invasion of privacy? What if the person accessing it was a government investigator or the storage service's administrator? Would that be a violation of privacy and would it be considered hacking? While the gut reaction to that question would be yes! a closer look would come out a little less clear.

The Fourth Amendment conceives of personal assets in physical terms – your house, your belongings, and your person. But in the case of the net storage service, the information is located far from your house on a machine which the 'hacker' was completely authorized to access.<sup>31</sup> So while the information would still be considered protected from criminal hackers, it is harder for the administrator or other authorized person to be considered hackers in the illegal sense.

People have surprisingly different views on privacy rights and no solution makes everyone happy. Some are in favor of the constant free flow of information – anything you want to know at the touch of a button.<sup>32</sup> Others are stingy with their information, not wanting to give out even their email address to register for a newsletter. There must be a delicate balance between too much privacy and too little – for some not even a balance at all but a losing war against technology. There are also many different takes on how much the government should regulate privacy.<sup>33</sup> But hacking a physical computer is an invasion of privacy; by compromising the machine, the hacker has compromised all the people who had data stored on that machine.

## **2.6 – Information Privacy**

---

<sup>31</sup> DeVries.

<sup>32</sup> <http://www.eff.org/> and <http://www.fff.org/> are two organizations dedicated to freedom of information.

<sup>33</sup> <http://www.epic.org/>



Privacy law can be divided into two conceptual areas. The right to be let alone, not to have a house searched without a warrant, and not to have belongings tampered with is one part of privacy law. This right covers the physical hardware of computers, your household desktops and networks, and information stored on removable media, such as CDs, within your house. This is what most people conceive of as traditional Fourth Amendment protection discussed in the last section.

Many people also expect to have the right to private personal information. Many people feel, for example, that the patient medical records kept by doctors should be completely private. Others feel differently, believing that a free exchange of information is important. Recently, the idea of having centralized medical databases where all the doctors in a geographic area, such as a city, could upload their records to a single location has become a popular concept.<sup>34</sup> The IT people could take care of the hardware, keep backups, and make sure things ran smoothly, removing the responsibility for security from the hands of the doctors. In addition, any doctor could pull a patient's records and save some time in asking for their medical history or having another office fax the records. This would allow patients coming in for emergencies to receive quicker care. It was in essence a proposal for freedom of information exchange.

There are two responses to this proposal – one from those in favor of freedom of information and another from those in favor of privacy. Those who tend to be interested in integration and ease of information access tend to think it a brilliant idea that would save time, trouble and possibly lives. Others rebel at the idea that personal information would be so easily

---

<sup>34</sup> <http://www2.clarku.edu/research/access/philosophy/decew/decewD.shtml>,  
<http://www.marketwatch.com/news/archivedStory.asp?archive=true&dist=ArchiveSplash&siteid=mktw&guid=%7BA337E62E%2D76E6%2D4343%2DB960%2D3F640D419DBF%7D&returnURL=%2Fnews%2Fstory%2Easp%3Fguid%3D%7BA337E62E%2D76E6%2D4343%2DB960%2D3F640D419DBF%7D%26siteid%3Dmktw%26dist%3D%26archive%3Dtrue%26param%3Darchive%26garden%3D%26minisite%3D,>  
<http://doctorisin.blogspot.com/2004/10/chips-are-down.html>



accessible. Even with privacy restrictions put in place so that a doctor could not access information without a patient's consent, having all that sensitive information stored in a central location makes it a target for hackers and for non-ethical doctors who figure they will never be caught. Many entities require personal information to operate; banks, schools and most businesses collect information to facilitate their day-to-day operations and each of these collections becomes a target for hackers. Considering the growing threat of identity theft through credit fraud, imagine if someone got access to medical records and were able to manipulate them or sell them. Both sides of the debate provide valid points. Deciding where the balance should be found is a difficult question still being debated.

In his book *Code and Other Laws of Cyberspace*, Lawrence Lessig gives an example of two college campuses that treat the idea of freedom of information in totally different ways. The University of Chicago supports complete anonymous access to the Internet by anyone who connects to their network. This policy was constructed by Geoffrey Stone, who was "a prominent free speech scholar" and claimed that the First Amendment grants the right to communicate freely without regulation. Harvard is the second example, where you have to register your computer and "all interactions with the network are monitored and identified to a particular machine," restricting the ability of students to conduct anonymous activities on the Internet.<sup>35</sup> These two different access policies were created with different goals in mind. One promotes the freedom of information, while the other promotes complete security. Lessig argues that networks can be regulated as much or as little as we choose for them to be; the issue is in the choice between privacy and security.

The privacy of information can also be critical to *preventing* computer intrusion. At a recent Blackhat Briefing, Cisco researcher Michael Lynn spilled information about bugs in Cisco

---

<sup>35</sup> Lessig.



routers – information that would allow hackers to exploit networks using Cisco’s hardware worldwide.<sup>36</sup> Cisco tried to stop Lynn’s talking and keep the information from malicious hands. While a patch for the security flaw Lynn mentioned had been released a few months earlier, net administrators are often slow to install patches and many systems were still vulnerable to the hackers who took the call to exploit the spilled information.<sup>37</sup> This spill of protected information will cause, at the very least, many attempts and perhaps some successful hacking of systems which have not yet patched this flaw. Because of a public leak of information, a vulnerability was brought to the attention of hackers who may otherwise have not paid attention. Information privacy concerns everyone. One known security flaw can become a weakness to any number of systems that house untold amounts of critical information.

Hacking involves access to information people want to keep private. If there were no privacy of information, there would be fewer stigmas against hacking for information, though hackers could still use their skills to create other kinds of havoc. But all this is just looking at what the public thinks about hacking – the hackers themselves, while often exploiting the information they get from their conquests, are often more interested in the difficulties involved in getting that information.<sup>38</sup> Compromising protected information is only one aspect of what hackers do, but it is a major part of what makes hacking illegal and so it is worth looking into further.

## 2.7 – Identity Theft

---

<sup>36</sup> “Black Hat is a think tank of security experts providing consulting, training, and briefings to corporations and government agencies around the world. The Black Hat team has experience working with organizations such as Amazon, DARPA, Microsoft, and the NSA.” <<http://www.blackhat.com/html/bh-about/bh-about-index.html>> Accessed 9.12.05.

<sup>37</sup> ‘Cisco struggles to plug net leak.’ *BBC News Online*. <<http://news.bbc.co.uk/2/hi/technology/4734415.stm>> Accessed August 1, 2005.

<sup>38</sup> Erickson, Jon. *Hacking: The Art of Exploitation*. No Starch Press, San Francisco; 2003. pp 1.



This concern over privacy, the obsession with security, and our attempts to protect ourselves from hackers is, in part, caused by a fear of identity theft, which occurs when someone steals personal information and uses it to commit fraud.<sup>39</sup> If someone gets a portion of relevant information about their victims such as credit numbers or bank account information, then they have access to their victim's money, history and credentials. Then the hacker can, for whatever purpose, take on the identity of their target. They can spend that person's money, use his credentials, and digitally impersonate him.

In 1998, the US government passed the Identity Theft and Assumption Deterrence Act, which defines the crime of identity theft and outlines punishment of up to 15 years in prison, fines and forfeiture of property.<sup>40</sup> Since then, companies have begun putting their own policies in place to help protect their customers from identity theft. Credit card companies and banks actively advertise their various forms of protection against identity theft. Commercials, banners, slogans and brochures all proclaim the safety of this or that service and tout their commitment to customer protection. They use company policy and network security measures to ensure their promises. Citibank created a series of commercials advertising their solution to the growing problem of identity theft.<sup>41</sup> They promise that customers will never have to pay for unauthorized charges and offer virtual account numbers to use in online transactions. Citibank also touts the security of their site and their team of internet security specialists.<sup>42</sup> By being upfront about the problem, Citibank hopes to attract customers scared of becoming victims and looking for the best protection, something which Citibank claims to be offering.

---

<sup>39</sup> <http://www.consumer.gov/idtheft/> Accessed 9.21.05.

<sup>40</sup> Public Law 105-318, 105th Congress <[http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105\\_cong\\_public\\_laws&docid=publ318.105](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=publ318.105)> Accessed 9.21.05.

<sup>41</sup> <http://www.citibank.com/us/cards/cardserv/advice/index.htm> Accessed 9.21.05.

<sup>42</sup> <http://www.citibank.com/us/cards/cardserv/advice/protect.htm> Accessed 9.21.05



Less obvious types of identity theft exist than credit card fraud. Any piece of digital information can be stolen, and the stealing can be as easy as knowing someone's social security number. In his book, *The Art of Deception: Controlling the Human Element of Security*, on the "art of social engineering," well-known hacker Kevin Mitnik relates several stories which involve hacking to allow the attacker to use the victim's identity in rather unusual ways.<sup>43</sup> Mitnik tells the story of a young man who hacked into a University's student records in order to find a graduate with the same name as his own. He was then able to use the graduate's social security number on employment forms so that, when the firm checked with the university, it would show he had a degree in Computer Science without him actually having to take the time to earn the degree.<sup>44</sup> The victim probably never even realized that his identity had been stolen to help another person get a job.

Another form of identity theft is to use another network for cover during a crime. Hackers will often route their attacks through other computers in an attempt to cover their tracks. They effectively use the identity of the secondary system to mask their own.<sup>45</sup> Many companies will uncover a hacking attempt that claims it came from an elementary school or an unsuspecting user. The company must then work with the secondary system's administrators in order to track the hacker.

Identity theft is only one of the problems which has become more common with the rise of the Internet and digital crime. Maintaining good security and being careful is one way to combat this form of theft, but one must also be vigilant to assure they have not been victimized. Hackers are always coming up with new ways to defeat the system and security researchers must

---

<sup>43</sup> Considered one of the most famous and wily criminal hackers to be jailed and convicted, he was charged with breaking into countless computers and now runs a security firm. <<http://www.takedown.com/bio/mitnick.html>>

<sup>44</sup> Mitnick pp 124 – 128.

<sup>45</sup> Kerr, Orin S. "Internet Surveillance Law After the USA Patriot Act: The Big Brother that Isn't." *Northwestern University Law Review*. 97 Nw. U.L. Rev. 607. Winter, 2003. Pp 662.



remain aware of the latest information and even try to outthink the hackers in order to best protect users.

## 2.8 – Legal Hacking

There is such a thing as legal or white-hat hacking. It occurs when the hacker is authorized to access the computers he is breaking into. It is hacking to check one's own system for security flaws. It is hacking to discover how to beat the hackers at their own game. It is generally self-preservation hacking. Almost any time I mention to a system administrator that I am doing my honors project on hacking, they happily sent me lists of links, books, and other resources they have stored up. Why are these system administrators so well versed in the subject of hacking, and more importantly, hacker-prevention? Well, there is a possibility a few of them actually *did* some less-than-legal hacking in the past. But for the most part the best way to protect the network for which they are responsible is to be *aware* of hacker methods and the latest attacks in order to combat them.

Take the Honeynet Project as an example of legal hacking.<sup>46</sup> Their aim is to provide research into computer defense, raise awareness of threats to computer security and teach those who are interested about defending networks against hacking. They provide information not only on the tools used by hackers, but also on the motives behind the attacks. Project Honeynet supports increased awareness as the best defense against hackers and has on their site a series of articles which argue that in order to “help protect [your] resources, you need to know who your threat is and how they are going to attack.”<sup>47</sup> By organizing security research from around the world, these security researchers are able to provide comprehensive resources for digital security and information on hackers and their methods.

---

<sup>46</sup> <http://project.honeynet.org/>

<sup>47</sup> “Know Your Enemy: The Tools and Methodologies of the Script Kiddie.” Honeynet Project. Last Modified: 21 July, 2000. Accessed 9.7.05. <<http://project.honeynet.org/papers/enemy/index.html>>



Their recent paper on phishing attacks, researched by the German and UK HoneyNet Projects, describes in detail the methods used to carry out phishing.<sup>48</sup> It is likely that almost anyone who receives spam has been the target of a phishing attack. A well-known online service such as PayPal is used as a front and the user is asked to reconfirm some details to keep their account active. If the user falls for the scam and actually sends their information, they have become a victim of a phishing scam. This sort of scam provides the hackers useful information with almost no work needed to access their bank accounts or other sensitive data. It is this sort of attack that Project HoneyNet aims to increase awareness of in order to defeat.

Project HoneyNet is just one example of a group dedicated to promoting system security. Many companies, governments and universities sponsor their own security research groups. UC Davis has a facility dedicated to computer security research, the European Union promotes security research on a coordinated basis throughout Europe, and the US Computer Emergency Response Team (US-CERT) helps coordinate “defense against and response to cyber attacks” within the US.<sup>49</sup> Each of these groups and many others add their voices to promoting system security. These groups can run hacking experiments on closed networks to learn new methods. This would be legal hacking, which comprises one important part of the defense against hackers, trying to figure out and fix the weaknesses before the malicious hackers find them.

## 2.9 – Summary / Conclusion

---

<sup>48</sup> “Phishing is the practice of sending out fake emails, or spam, written to appear as if they have been sent by banks or other reputable organizations, with the intent of luring the recipient into revealing sensitive information such as usernames, passwords, account IDs, ATM PINs or credit card details. Typically, phishing attacks will direct the recipient to a web page designed to mimic a target organization’s own visual identity and to harvest the user’s personal information, often leaving the victim unaware of the attack. Obtaining this type of personal data is attractive to blackhats because it allows an attacker to impersonate their victims and make fraudulent financial transactions. Victims often suffer significant financial losses or have their entire identity stolen, usually for criminal purposes.” “Know your Enemy: Phishing Behind the Scenes of Phishing Attacks.” The HoneyNet Project & Research Alliance. Last Modified: 16th May 2005. Accessed 9.7.05 < <http://project.honeynet.org/papers/phishing/> >

<sup>49</sup> <http://seclab.cs.ucdavis.edu/index.html>, [http://europa.eu.int/comm/enterprise/security/index\\_en.htm](http://europa.eu.int/comm/enterprise/security/index_en.htm), <http://www.cordis.lu/security/>, <http://www.us-cert.gov/aboutus.html> Accessed 9.8.05



Whether they prefer to be called hacktivists, security experts, intrusion specialists, script kiddies or spammers, the actions of people who break into computers can be referred to as hacking. For some, this is a legal exercise undertaken to gain knowledge about hacking in general or in order to learn their system's vulnerabilities. For others, it is a game to see who can hack past the strongest security. And for some, it is a means to an end, acquiring information or crashing a system.

The past few sections have given a brief overview of the current state of the world of hacking, both legal and illegal, mainly by looking at what hackers do and how prevalent they are becoming. It has also raised some of the legal questions which will be looked at in more depth in section four. Next we are going to delve far deeper into the world of hacking to meet the hackers themselves. The focus will not be on what they do as this section was, but whether on who they are and why they hack.



## Section 3 – Who are the Hackers?

### 3.1 Introduction – Types of Hackers

Today's hackers are a curious and diverse bunch. If an apple a day keeps the doctor away, a hack a day<sup>50</sup> provides a great diversion for hackers with nothing better to do and a curiosity about hacking everything from Xboxes to cell phones and iPods to GPS units. The website Hackaday.com contains computer hack tutorials covering subjects such as how to hack network printers<sup>51</sup> and how to embed a WiFi detector in a backpack strap.<sup>52</sup> Some of the hacks describe changes that can be used to make your own computer better, while others have more sinister applications. As the site claims, their hacks have "so much potential to be used in good *and* bad ways."<sup>53</sup> The site provides links and information for anyone interested in hacking without regard to how it will be used. While the site tends to feature the how-to aspect of hacking as well as more hands-on projects, the site archives are full of useful information for the curious and malicious.

Other hacking sites focus more on the network security issues involved in protecting a network from hackers. These sites list not only the newest hacks, but ways to protect your system against these hacks. SecurityFocus.com is one example of such a website. They provide news and research on cross-vendor security issues ranging from Mozilla's Firefox web browser<sup>54</sup> to Microsoft's security patches. SecurityFocus is owned by Symantec but attempts to remain vendor neutral by reporting on security breaches and patches across all platforms and for all programs. Microsoft, for example, recently canceled a security update concerning the Windows operating system. This had security gurus questioning whether the lack of a patch left them open

---

<sup>50</sup> <http://www.hackaday.com> <Accessed 9.14.05>.

<sup>51</sup> Eliot Phillips <http://www.hackaday.com/entry/1234000100058731/> <Accessed 9.14.05>.

<sup>52</sup> Fabienne Serriere <http://www.hackaday.com/entry/1234000683058639/> <Accessed 9.14.05>.

<sup>53</sup> Vince Veneziani <http://wireless.hackaday.com/> <Accessed 9.14.05>.

<sup>54</sup> John Leyden, The Register 2005-09-12. <http://www.securityfocus.com/news/11309> <Accessed 9.15.05>



to attack on what had become a known and published weakness.<sup>55</sup> While they tend to report significantly more Windows vulnerabilities, there are plenty of reports concerning Apple computers, Unix systems, and even computer forensics. Security specialist sites tend to focus less on the possible exploits and more on the latest patches and fixes for deterring exploits. While less information exists on *how* to breach the security, these sites try to put their focus on *fixing* the problems and preventing future attacks. For a malicious hacker, though, the list of problems which have been recently discovered is an excellent resource of vulnerabilities that have recently been fixed or not fixed at all.

In-between the white- and black-hat sites are those focused on a specific type of hacking. They would include, for example, the hacktivist websites run by a sub-set of hackers who see their mission as spreading information (or misinformation). They do so by defacing public websites. "Hacktivism" can be defined as "a policy of hacking [...] to achieve a political or social goal"<sup>56</sup> and is generally carried out via electronic civil disobedience, the breaking into a computer (hacking) for a specific political or ideological purpose and leaving behind a message. These hackers are not black-hat in the sense that they are not stealing information or crashing systems, nor are they white-hat, though they often try to help the sites they hack by offering patches for the security holes they exploit. Their actions are illegal in that they gain unauthorized access, but they see themselves as promoting freedom of speech.<sup>57</sup> In 1998, for example, a hacktivist known as Milw0rm broke into the computer system at India's Bhabha Atomic Research Centre in Bombay as a protest against nuclear weapons tests. While the hacktivists view their actions as a form of expression, the companies whose sites get broken into have different views.

---

<sup>55</sup> Robert Lemos, SecurityFocus 2005-09-13, <http://www.securityfocus.com/news/11313> <Accessed 9.15.05>

<sup>56</sup> <http://www.thehacktivist.com/hacktivism.php> <Accessed 9.15.05> Written by metac0m (December 2003).

<sup>57</sup> Ibid.



In December 2000, 17 year old Robert Lyttle, known across the Internet as “Pimpshiz,” was arrested for a large number of hacktivist attacks defacing websites in support of the file-sharing program Napster (not the current, legal Napster but its earlier version that was widely known for illegal file sharing). From NASA’s website to Don Henley’s homepage, Pimpshiz hacked into web servers and left behind his pro-Napster message and an offer to help patch the security holes he had exploited.<sup>58</sup> He was eventually caught, plead guilty and was given a restitution payment and restricted from using the Internet. But this has not stopped him from starting his own security company called SubSeven Software and speaking out about the usefulness of hackers. He claims that hackers are helpful to system administrators, forcing them to keep their networks updated. Pimpshiz is a good example of a hacktivist, a clever hacker with a message to spread and the opinion that he is right in doing so. Even though he has been prosecuted for his actions, he still speaks of his actions as a good but misunderstood occupation.

In a 2004 statistical analysis of hackers who were convicted of computer crimes, I was able to establish a basic demographic profile for a hacker. 86% male, and largely between the ages of 18-25 (though there were significant portions older), only 3% were juveniles and 3% women. Their sentences seemed to focus either in prison or house detention and a fine as well as losing their computer access for a period. Looking over newer cases shows that trends in computer crimes are still changing. While the basic demographic may remain the same, the result of the hacking has shifted from crashing a network to crimes like identity theft and phishing and creating zombie computers (though this last generally involves an attempt to crash a network elsewhere, so maybe hackers have not changed that much after all).

---

<sup>58</sup> McManis, Sam. ‘An Internet outlaw goes on record; Pleasant Hill student tells of his ‘hacktivism’.’ *San Francisco Chronicle*, Feb 24, 2002.



Information on how to compromise almost any type of system is widely available on the Internet; how a hacker chooses to use this information is what defines them as black-hat or white-hat. The level of skill required to hack ranges from the very novice script kiddies who use other people's work (their "scripts") to exploit vulnerable networks to the expert programmers who hack the most secure networks or send out highly destructive viruses. Some hack to help expose flaws in systems, some hack to gain information, and some hack for political causes. Each type of hacker is interested in information, whether it is acquiring private information, spreading a message, destroying information, or just figuring out how hacking is accomplished. Script kiddies, black-hat hackers, virus writers and white-hat security specialists each have their own interests, their own net communities, and their own goals. Their communities, while varied, carry similar sorts of information. What ties them all together is their hacking and exploitation, legal and illegal, and their desire to learn more.

### 3.2 Script Kiddies

The script kiddie is generally considered a novice hacker, "the hacker looking for the easy kill."<sup>59</sup> While it could be a skilled hacker trolling a network for a certain vulnerability, the person using the pre-packaged hack is normally trolling a large chunk of the Internet looking for a network with the vulnerability they want to exploit – the easy kill. Generally, this hacker only knows how to do a small number of "exploits," or hacks, and surfs the Internet looking for systems vulnerable to these attacks. Since these scans are random, there is a good chance almost every system has been probed for these common weaknesses. Once the kiddie finds the specific weakness he is looking for, he is able to hack the system and gain various levels of access depending on what the exploit was designed to do. The best protection against script kiddies is

---

<sup>59</sup> "Know Your Enemy : The Tools and Methodologies of the Script Kiddie" The Honeynet Project. <<http://project.honeynet.org/papers/enemy/index.html>> Published 7.21.00. Accessed 9.19.05.



keeping track of updates and security patches for all computers connected to the Internet. With so many scripts easily available to so many people, there are large numbers of script kiddies randomly scanning the Internet looking for vulnerabilities. Even new and obscure systems are scanned for weakness since the scans are random and run over all ranges of addresses without regard to how new or well-known the networks they are exploiting. There is no security through obscurity when dealing with the script kiddie; security comes only through vigilant updating.

Finding the tools necessary to exploit computers is as simple as searching the Internet with a good search engine. Password crackers to help break various system passwords are freely available; one for Windows can be found at [osid.it](http://osid.it). While the author claims it is only for ethical uses,<sup>60</sup> it could just as easily be put towards illegal ones. There are several other tools available on the Internet tailored to different operating systems and tools for general purpose password cracking. One of the best-known such password crackers is John the Ripper,<sup>61</sup> a Unix-based password cracker available free to download from the web. Getting the right tools is the first step to hacking as a script kiddie.

Script kiddies use exploits, or pre-programmed hacks (hence scripts), which are free and found on many websites across the Internet, both the security-focused and hacking-focused websites. One example of such a page is Hoobie.net, which features a collection of simple exploits that can be downloaded and run by anyone interested. Such exploits include, for example, a file that can be put on a computer running Windows NT to collect passwords,<sup>62</sup> an

---

<sup>60</sup> <http://www.osid.it/cain.html>> "Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols. The program does not exploit any software vulnerabilities or bugs that could not be fixed with little effort. [...] The author will not help or support any illegal activity done with this program."

<sup>61</sup> <http://www.openwall.com/john/>

<sup>62</sup> <http://www.hoobie.net/security/exploits/hacking/ntpwgrabber.txt>



exploit for crashing Windows,<sup>63</sup> and several others designed to freeze systems due to overflow. Each of these exploits has a script (program) which can be used by the hacker so that he does not have to write the code himself. For example, the password-collecting exploit contained a .txt file which would be saved into the /system32 directory as a .dll file. Once the hacker gained access to the computer, he could simply store the file in the correct location and come back later to pick up his passwords. It would not be necessary for him to take the time to program the file himself. Someone else has already done that and provided it to him.

Buffer overflow is a common type of weaknesses exploited by script kiddies and is a useful trick for crashing a system and creating total havoc. Crashing a system is easily accomplished through a programming error in the system that leads to an error referred to as buffer overflow. This occurs when more information is written to a section of memory than it has space to hold.<sup>64</sup> For example, the program tries to write a larger number or longer string of text than the program has space to hold. This technique can be used either to direct the program to another bit of code spliced in at a different location or to crash the computer by putting it in a repetitive cycle where it cannot find its next instruction. Security updates very often patch overflow errors made by the programmers in the initial release of the code. In a recent update released for Macintosh computers, four of the six listed vulnerabilities the patch fixed could lead to buffer overflows.<sup>65</sup> Since this is so common and easy to find and use, it is little wonder that many exploits script kiddies engage in feature crashing systems using buffer overflow.

Script kiddies are the babies of the hacking community. They cause trouble on less-than-secure systems and encourage vigilant updating on others. But they are learning about computers

---

<sup>63</sup> <http://www.hoobie.net/security/exploits/hacking/land.c>

<sup>64</sup> Erickson pp 22.

<sup>65</sup> US-CERT, Technical Cyber Security Alert TA05-229A, Apple Mac Products are Affected by Multiple Vulnerabilities <<http://www.us-cert.gov/cas/techalerts/TA05-229A.html>> Posted 8.17.05. Accessed 9.19.05.



and their weaknesses. They can stop, or only hack on their own systems, or they can continue to learn and develop their hacking skills for use on more and more sophisticated networks.

### 3.3 Black-Hat Hacking

Far more knowledgeable about computers than those who just use scripts to hack randomly into weak networks are the hacker elite, the skilled, knowledgeable and clever experienced hackers. And these people sometimes use their skills for less than legal purposes. They differentiate themselves from the rest of the hacker-world by names such as black-hat hackers, crackers, or just attackers.<sup>66</sup> Many legal hackers get very offended that these criminally minded people are commonly labeled with a term they consider to be a compliment.<sup>67</sup> The black-hat hacker can be anyone, not just some teenaged kid out to hack for fun, but the hacktivists discussed above, disgruntled employees seeking revenge, the competition looking for an advantage; anyone with a desire to uncover protected information and the skills to do so.<sup>68</sup> Even though their activities are illegal since the machines they are accessing are protected, people still engage in hacking. They believe they will never be caught if they are sneaky about how they enter and careful about covering their tracks as they leave. The criminal hacker must be extra-careful, but the process is simple detection and exploitation.

A good hacker will start by learning as much about his intended target as possible. Every detail is important to a successful hack. Some people call this reconnaissance;<sup>69</sup> others call it footprinting.<sup>70</sup> But the idea is still the same – to gather information about your target’s network and settings. The more the hacker knows about a network, the more vulnerabilities he will be

---

<sup>66</sup> Skoudis pp 10.

<sup>67</sup> Raymond, Eric Steven. “How to Become a Hacker.” <<http://www.catb.org/~esr/faqs/hacker-howto.html>> Accessed 10.5.05.

<sup>68</sup> Raymond pp 7-8.

<sup>69</sup> Raymond pp 145.

<sup>70</sup> McClure pp 6.



able to exploit. A Whois search can reveal details such as contact information, geographic location, and IP addresses.<sup>71</sup> A traceroute on the IP address can show how the information is being routed to and from the system. Ping sweeps determine which portions of the network are active.<sup>72</sup> Port scans look for unprotected ports. Further tools allow a hacker to form a very good picture of the network's structure and security. Each of these techniques requires little more than a net connection and are non-invasive so the target network never notices the probing.

Different types of systems have different weaknesses that are commonly exploited. Some weaknesses are in the system's code, others lie in the programs a system runs, and still more can be found in the protocols one machine uses to communicate with another. Windows, as the most popular operating system on the market today, is also the one most commonly exploited. Most viruses are written for Windows machines, and since many computers run one version or another, hackers spend a lot of time and energy looking for ways to compromise this particular operating system. While Microsoft is diligent about posting fixes for problems as they are discovered, users are often slower about installing the updates which leaves their systems vulnerable to publicized threats.<sup>73</sup> Unix systems such as Linux are another common target of hackers. Developed in an open-source manner (meaning the code is available to anyone and updates can be made by anyone), Unix systems tend to have good security, as users discover and post fixes to the code.<sup>74</sup> But there are still vulnerabilities that can be exploited using the various protocols by which the system connects to the Internet.<sup>75</sup> And finding a clever way to exploit a Unix machine (and posting the fix) can be a source of much praise in the programming community. Even Macintosh computers (which are based on Unix), websites, wireless networks

---

<sup>71</sup> Skoudis pp 162.

<sup>72</sup> McClure pp 42.

<sup>73</sup> McClure pp 140.

<sup>74</sup> McClure pp 212.

<sup>75</sup> McClure pps 216-272.



and various other applications are targets for hackers. A hacker will discover what software and protocols are run on a certain machine and then be able to tailor his attacks to the common weaknesses of that system.

When they get inside the system they were hacking, the damage these malicious hackers can create is incredible. They can not only view information, but also change it, delete it or corrupt it. They can change the structure of a network, hide important files, and change passwords, all actions that generally create havoc for users. While for some hackers, the goal is simply to acquire protected information, many others just want to make as big a mess as possible. They often accomplish this by releasing a virus onto the compromised network. As with other tools, viruses are freely available online for download and use and are an excellent tool for creating havoc and gathering information.

### **3.4 Bad Code: Viruses, Bugs and other malware**

Another form of invasive information gathering that can be used in conjunction with hacking is malicious code: viruses, worms, and Trojans. While these unpleasant little programs can be distributed in emails or downloaded from the web, they can also be implemented by a hacker in order to keep a backdoor to a system open or to exploit information the system may have or to just make a mess.

Worms are typically able to run themselves without needing any application to latch onto; they are independent programs, which can execute independently. They mainly replicate across networks, going from computer to computer and affecting as many different machines as possible. Like their natural counterpart, code worms burrow through a system leaving damage in their wake and burrowing onwards.



Viruses have the potential to evolve and replicate themselves within a host system. They infect a single computer and spread within it before moving to further computers. They spread using email and the Internet (and now messenger programs) as well as vulnerabilities on servers. Virus research is a quickly developing field as new and sophisticated viruses are released regularly. Even adaptations of older viruses can cause a mess if a user does not get regular updates to their anti-virus software. And since viruses replicate themselves within a host, a single computer could contain several unique instances of a particular virus.

Trojans, called after the legendary Trojan horse of Homer, are the most common tool used by hackers because of their simplicity and the ease with which they escape detection.<sup>76</sup> A malicious piece of code, the Trojan is attached to a legitimate program which the victim or hacker runs. When the program is started, the malicious code also starts and creates a backdoor into the system or gathers information or steals passwords or does whatever the programmer designed the Trojan to do. These codes can be used by hackers to gain access to a system by sending them to unsuspecting users and hoping the user runs the legitimate program which installs the Trojan. Or they can be installed later by the hacker to gain whatever functionality the program has and hide behind the mask of the legitimate program so the user does not remove the Trojan.

There are other kinds of malicious scripts that are less-well-known such as logic bombs built into an application and set to go off after a certain amount of time or at a certain trigger, spam programs which flood the victim with unsolicited emails, flooders, keyloggers, and joke

---

<sup>76</sup> McClure pp 31.



programs.<sup>77</sup> Each of these malicious scripts can be used to infiltrate a system and give the hacker who introduced the program some advantage or information.

Even with careful protection, viruses infect computers regularly and new viruses are released almost daily. October 12, 2005 saw the release of a new Trojan for Windows computers called Backdoor.Graybird.R. While not considered much of a threat by itself, it hides itself on the victim's computer and proceeds to download files onto their hard drive. This can allow hackers to install further programs onto the computer or gather personal information about the user.<sup>78</sup> New viruses are released almost every day, sometimes multiple viruses are released at the same time. Norton released five updates on October 12, two the day before and six on October 7, showing how frequently one has to update to keep systems completely protected from potential threats.

Malicious codes are a tool used by even expert hackers to extract the information they need from a computer with minimal effort. While not all virus attacks are intentionally caused by hackers, many unintentional ones, if not corrected, can leave doors open on a system that can be exploited by a script kiddie or black-hat hacker or fixed by a white-hat security specialist.

### **3.5 Helpful Hackers (white hat), Security specialists**

Every book, website, and article on hacking has a caveat; to learn the provided information and then use it to *defeat* hackers and protect your own network. "Of course," writes Peter Szor in his book on virus research, "the knowledge of computer viruses is like the 'Force' in *Star Wars*. Depending on the user of the 'Force,' the knowledge can turn to good or evil. I

---

<sup>77</sup> Szor, Peter. *The Art of Computer Virus Research and Defense*. Addison-Wesley, Upper Saddle River, NJ; 2005. pps 28-38.

<sup>78</sup> <http://securityresponse.symantec.com/avcenter/venc/data/backdoor.graybird.r.html> Updated 10.12.05 Accessed 10.12.05.



cannot force you to stay away from the 'Dark Side,' but I urge you to do so."<sup>79</sup> Similar pleas echo in each book on hacking; here is my knowledge, please use it for good. And certain people use the information and hack to help learn how to prevent unwanted intrusion. These people are the white-hat hackers, the security specialists, the intrusion specialists; sometimes even a net administrator will hack his system to check for weaknesses and figure out where patches are needed. These hackers have permission to access the systems they are hacking and so are the legal hackers.

Many IT companies employ people whose job is specifically to try and hack into various different setups and share their findings both to increase the effectiveness of their company's product as well as increasing the general knowledge available about the weakness. McAfee's Foundstone Security Training offers programs specifically designed for network administrators who want to learn how to keep hackers off their networks and how to write secure software.<sup>80</sup> These programs teach basic hacker awareness as well as how to stay up-to-date in this changing field and how to implement the most effective security.

There are also independent groups who hack to find and report weaknesses; these groups are careful not to hack where they are not supposed to. They set up test networks and then try and find all the weaknesses hackers might exploit. This would be a group like the Honeypot projects mentioned earlier. These groups are not vendor-specific. Rather, they are interested in solving particularly complicated problems that have yet to be exposed.

The white-hat hackers are on a search for knowledge that can be used to defeat the black-hat hackers and increase overall security. While both groups develop the same skills, each has a different goal in mind. Network security against illegal hacking is the goal of white-hat hackers:

---

<sup>79</sup> Ibid xxiv.

<sup>80</sup> [http://www.mcafeesecurity.com/us/services/education/mcafee/classroom\\_training/foundstone.htm](http://www.mcafeesecurity.com/us/services/education/mcafee/classroom_training/foundstone.htm) Accessed 10.12.05



to find and fix holes before the black-hat hackers can exploit those vulnerabilities.

### 3.6 Hacker Forums

Gathering in communities to share information discovered during exploits is one way hackers, both good and bad, exchange techniques. They also use these forums to teach newbies (new hackers) and brag about their latest exploits to gain prestige within their community. Some of these communities are informal groups that meet regularly in chat rooms such as IRC or spread on newsgroups; others are far vaster and publish online articles and printed newsletters and even arrange hacker conventions. Some of these sites are well-established; others are hard to find as they move from server to server and location to location. Links that were active one day are broken the next as the community moves around, and those who are not regular members may find it hard to keep up with these changing locations.

*2600: The Hacker Quarterly*, named after the alt.2600 newsgroup where hackers are known to congregate, can be found in many larger bookstores and carries such articles as “Hacking Google Map's Satellite Imagery,” “Home Depot's Lousy Security,” and “Creating AIM Mayhem.”<sup>81</sup> The articles explore different hacks, explain new technology developments, and share problems and solutions among the different participants who write in to share their observations and suggestions.

*HackWire*, a news website updated frequently by its various users, provides another source of hacker news and information. As a repository of hacker-related news, it carry links to articles on the latest exploits, new viruses, hackers who are standing trial and recent hacking successes. For example, it reported on the recent successful hack of Microsoft's website which

---

<sup>81</sup> Summer 2005 Issue <<http://store.2600.com/summer2005.html>> Accessed 10.3.05



was defaced with a graphic saying “Free Rafia – Hack is not a crime.”<sup>82</sup> These articles include comments added by users who use the space to do everything from advertise their own hacking expertise to expounding upon the article and offering further resources to helping interested people look into both how to exploit the hack or how to patch it. HackWire was rated as the #3 hacker underground site by Underground100<sup>83</sup> and the top hacker news source as of August 17, 2005.

These forums are useful sources of information on trends within the hacker community. By exploring them, one can see what new systems they are looking to exploit, what they find easy and what types of exploits are more complicated, what their recent successes are and the most popular methods they are exploiting. These sites show the hackers’ curiosity, their intentions and can be used to find information to test your system, see which vulnerabilities are the most popular and common and discover what sorts of systems the hackers are likely to start targeting next.

### **3.7 Summary / Conclusion**

Hacking is a search for new and inventive ways to exploit computers, whether to use that knowledge to gain illegal access or to learn how to fix their weaknesses. Hackers are interested in information, sharing it, acquiring it, and bragging about their clever uses of it. They gather on the Internet and in person to share their findings, to teach fellow hackers and advance the knowledge of hacking. Their insights lead to changes in technology from security patches to new releases to better security software and each new hack they find stirs interest and furthers awareness of computer security. Though their goals may differ, all hackers collect information to put to use and most gather in communities to share the information they have acquired.

---

<sup>82</sup> <http://www.hackwire.com/comments.php?catid=2&id=179> Posted 7.8.05 Accessed 10.3.05. Image can be seen at <http://www.cyber-army.org/microsoft.gif>

<sup>83</sup> <http://www.ug100.com/> Accessed 10.7.05.



But all this information raises a very important question, is this really who the hackers are or are they a more vague and indescribable group? Can we ever be completely sure of who they are, if they are in fact a specific group or are they perfectly normal humans who suddenly decide to use their skills for computer intrusion. Perhaps they are some of both. In either case, though, it makes security hard. The network administrators work tirelessly to keep their networks updated, but a skilled and determined hacker can still break through with enough time and patience. Network security is no guarantee of digital safety. But just as a seat-belt is a good guard, so security keeps out many unwanted intrusions. And good laws can control much of the intrusion on the net, though regulating everything would be impossible. The only truly safe computer is one which is locked in a closet connected to nothing. All other computers have to compromise their safety, just a bit, for the benefits gained by their access.



## Section 4 – What do we do about Hackers?

### 4.1 - Vulnerable Machines

While so far this paper has concentrated on computer hacking, it is important to mention that there is a wide range of electronic devices that can be exploited and used by the curious and knowledgeable hacker. Computer hacking may be what the media currently reports on most (though there has recently been a rise in the reports of cell phone hacks; a return to the early days when the primary targets of hackers or phone phreaks was telephones and telephone companies). But computer hacking is far from the only kind in existence.

This is what makes the hacker world so fascinating. It doesn't have to be just about computers and phones. In fact, it gets rather boring when that's all one focuses upon. Hacking is much bigger than one particular technology. It's a state of mind that can be applied to virtually anything. This is what the media and all the wannabes can never understand.<sup>84</sup>

Several of the websites mentioned in previous sections of this paper feature hacks for other forms of electronic equipment from radios to soda machines to GPS units. While they provide this information for educational purposes with the hopes that the company will develop a way to fix the security flaw, many readers report using the flaw for their own increased convenience. Hacking, they argue, is the state of mind a person has when they are figuring out a new or clever trick. So any electronic device that is changeable is subject to hacking.

Keyboards, for example, can be hacked two different ways. While the primary purpose would be to gain information for a further attack, few people would think that such a simple device as the basic keyboard can be in danger of being compromised. One method would be to use a keylogger program which simply recorded all keystrokes made from the time it was activated forward till the time it is checked for information. The hacker could then go back and look for username password combinations or at information put into the computer. The second

---

<sup>84</sup> 2600: *The Hacker Quarterly*. Volume 22 Number 2, Summer 2005. pp 38. Accessed 10.10.05.



method involves a little gadget called a Key Katcher<sup>85</sup> that is plugged in between the keyboard and computer. It also records all keystrokes but does not operate on the machine as a piece of software so a search of running programs would not reveal its existence. The user would have to check physical connections to notice the device. The hacker could come later and remove the gadget and dump all the keystrokes into a text file for his perusal, gathering the same sorts of information as the key logger program.

It goes without saying that personal computers and the equipment they use to connect to the network, such as servers, are vulnerable to attacks and are targets for hackers simply because of the information they store or the possible havoc they can wreak with access to these machines. But there are so many other simple electronic devices that can be hacked and exploited to the benefit of the hacker and the detriment of others. Faked barcodes<sup>86</sup> can be created and used for any number of applications where barcodes are employed (such as shopping, gift cards and even some companies which use the barcodes as their primary means of identification). While these barcodes seem innocuous, they can be used to gain access, either to money or information; whatever benefits the barcode is designed to grant the bearer.

A mobile infrared transmitter (MIRT)<sup>87</sup> is a gadget designed to hack stoplights. Tired of waiting on that red-light to turn green? Get one of these gadgets (illegal for unauthorized users due to the Safe Intersections Act)<sup>88</sup> and start breezing through town on all green lights. Designed for use in ambulances and fire trucks with a legitimate need to get to their destination quickly, they can be purchased off the Internet and used on a daily commute. While in response to this, traffic lights are being switched over to a coded signal, this still takes time, leaving a lot of traffic

---

<sup>85</sup> <http://www.thinkgeek.com/gadgets/electronic/5a05/> Accessed 10.10.05.

<sup>86</sup> <http://www.barcodeinc.com/generator/> Accessed 10.10.05.

<sup>87</sup> <http://www.sportsimportsltd.com/trlich.html> Accessed 10.10.05.

<sup>88</sup> Poulsen, Kevin. "Traffic Hackers Hit Red Light." *Wired News*. August 12, 2005. Accessed 10.10.05.



lights open to exploitation by this tool. This is a good example of a known problem with a fix, but where distributing that fix is time consuming and expensive and leaves unfixed stoplights open to exploitation by a well-known flaw.

Another gadget works like a universal remote, allowing the annoying hacker to turn off any TV within 50 feet in under a minute.<sup>89</sup> People have been hacking TVs and VCRs for years and the new TiVos are also targets for the experimentation and skills of hackers.<sup>90</sup> While the goals are generally personal and the changes only affect the user, they are often circumventing copyright protections and other legal restrictions designed to retain the rights of the copyright owners against just such events. And publishing this information online allows more users to hack their TiVos without having to figure out for themselves how it is done.

People have long been taking apart electronics and trying to change them for uses other than their intended purposes or to increase their performance. Curious computer geeks have long scavenged old computer parts and used them to overclock their system in an attempt to have the fastest and most powerful computer.<sup>91</sup> With the wide spread of electronic gadgets, this has simply become easier and more common. And with the advent of the Internet, hackers now have the ability to exploit electronics through software from all across the globe. Now software and other digital commodities such as music can be exploited by hackers, though they are protected under law by copyrights.

## 4.2 Copyright protection

The issue of copyright protection has received a lot of attention lately as the proliferation of programmable electronics such as computers makes it easy to copy digital files and the spread

---

<sup>89</sup> <http://www.thinkgeek.com/gadgets/electronic/755e/> Accessed 10.10.05.

<sup>90</sup> <http://www.keegan.org/jeff/tivo/hackingtivo.html> Accessed 10.10.05.

<sup>91</sup> <http://www.extremeoverclocking.com/> is one example of a site devoted to overclocking or taking a computer's hardware and pushing it to get the maximum performance – generally faster than factory recommended.



of the Internet makes sharing those files quick and easy. A program such as iTunes, whose network share function is designed for users to listen to other's music but not download and burn, is the type of file-sharing that artists like because it spreads their music while still preserving their rights to the works. But this method is hardly secure as coders have developed programs such as myTunes (PC) and ourTunes (Mac) that allow users to download music straight from other people's iTunes playlists and burn or further share the files.<sup>92</sup>

But even users who choose legal programs such as Napster discover these paid services have their drawbacks due to the copyright limitations they have to follow. Songs downloaded are limited to use on a certain number of computers and portable devices and often only allow the song to be burned to CD a limited number of times.<sup>93</sup> Once a certain playlist has been burned a certain number of times, the user will discover she is no longer able to burn copies, even for her own personal use, of music she purchased. Hackers are interested in circumventing these protections in order to acquire and further share the information (in this case, music) with other users and so build programs which allow file sharing of unprotected files and ripping of protected files.

In 1998, Congress passed the Digital Millennium Copyright Act (DMCA - HR 2281), an attempt to regulate copyrighted material on the Internet. It makes programs such as myTunes illegal because they are designed specifically to circumvent the copyright protections put in place by iTunes. The DMCA specifically protects the Internet Service Providers (ISPs) who are the unknowing conduits of illegal file sharing as long as these ISPs disable the offending sites and accounts when they are informed of their activities in violation of someone's copyright. This helps promote privacy as the ISPs do not have to constantly police their users, patrolling their

---

<sup>92</sup> <http://minimalverbosity.com/> Accessed 10.13.05., <http://ourtunes.sourceforge.net/> Accessed 10.13.05.

<sup>93</sup> Napster Terms and Conditions. <http://www.napster.com/terms.html> Accessed 10.13.05.



files for illegal material. But it also means that unaware ISPs may well host a significant amount of copyrighted information that has not been legally copied.

Some people argue that the DMCA hurts the music industry as it allows someone to be prosecuted for publishing information (in print or on the Internet) on how to break the various copyright protection schemes. But since that information exists (and some copyright programs are notoriously easy to crack) the industry weakens its on protection by not allowing for outside innovation.

Much of information exchanged over the internet is digital information, intellectual property that can be copyrighted and protected under the law. While the Recording Industry Association of America (RIAA) brings much attention to pilfered music that violates copyright, other works such as books, blueprints, paintings and even graphics can be copyrighted material which the creator has a right to the exclusive use of or compensation for.<sup>94</sup> Many people who believe information should be shared have banded together to form groups that share legal files and offer compromising methods of copyrighting files to those who wish to share their work but still retain rights to it.

The Creative Commons is one example of such a group, widely used on works published electronically on the web. Founded in 2001, Creative Commons endeavors to provide a sustainable middle ground of creative copyrights where the owner retains a degree of control, but files can be shared and certain uses can be encouraged.<sup>95</sup> Their goal is to promote sharing of artistic work so users can enjoy and even use other's work in the creation of their own.

Copyright protections do not stop determined hackers who see it as a challenge and develop programs to rip and share CDs and DVDs and methods to propagate the stolen

---

<sup>94</sup> <http://www.riaa.com>

<sup>95</sup> "About Us: Creative Commons." <http://creativecommons.org/about/history> Accessed 10.26.05.



information across the web. Every time copyright owners come out with new technology designed to protect their rights, hackers come up with ways to circumvent that protection and get the goods they are interested in.

#### 4.3 P2P and other file sharing networks

Illegally copied files fly across the Internet daily with services such as WinMX (which recently closed due to threats from the RIAA<sup>96</sup> and was then resurrected<sup>97</sup> by a group from TheSourceCode<sup>98</sup> who helped users connect to other nodes and share files), LimeWire<sup>99</sup> and filesharing protocols such as Bit Torrent<sup>100</sup> (which was not designed to be used for illegal filesharing, but nevertheless often is used for such through sites such as isohunt.com and torrentsproxy.com). These services spread files to millions of users who want the illegal goods. And while some of these files come from people who have bought the CD and ripped the music to enjoy and share, others come from hackers who have broken into a record company or movie production company and stolen their files.

It's a commonly held belief that P2P is about sharing files. It's an appealing, democratic notion: Consumers rip the movies and music they buy and post them online. But that's not quite how it works.

In reality, the number of files on the Net ripped from store-bought CDs, DVDs, and videogames is statistically negligible. People don't share what they buy; they share what is already being shared - the countless descendants of a single "Adam and Eve" file. Even this is probably stolen; pirates have infiltrated the entertainment industry and usually obtain and rip content long before the public ever has a chance to buy it.<sup>101</sup>

---

<sup>96</sup> Mennecke, Thomas. "WinMX PNP Network Mysteriously Ends Operations." Sept 21, 2005. <http://www.slyck.com/news.php?story=921> Accessed 10.16.05.

<sup>97</sup> Mennecke, Thomas. "Resurrecting WinMX." Sept 23, 2005. <http://www.slyck.com/news.php?story=925> Accessed 10.16.05.

<sup>98</sup> <http://www.thesourcecode.us/> Though this domain appears to lead to a front page and no further links.

<sup>99</sup> <http://www.limewire.com/english/content/home.shtml>

<sup>100</sup> <http://www.bittorrent.com/>

<sup>101</sup> Howe, Jeff. "The Shadow Internet." *Wired*. Jan 05. <http://www.wired.com/wired/archive/13.01/topsite.html> Accessed 10.16.05.



This is truer on networks such as LimeWire than the one accessed using myTunes. On a local network you are likely to find a much higher number of files people actually bought than files downloaded illegally or stolen. But these files found across the Internet are not always from hackers, sometimes they are from people who work within the music industry and smuggle the files to the pirates in return for other downloads.

In 2001, A&M Records sued the file-sharing program Napster for providing their service, which allowed transmitting of illegally obtained versions of its copyrighted music. Napster was forced to shut down until they could implement a method of filtering for copyrighted files.<sup>102</sup> This proved almost impossible to do, so Napster shut down for a year and reopened as a legal paid music download service.

The threat of legal action did not stop other file-sharing programs from taking over where Napster left off. Programs such as WinMX, which had always been around, experienced a surge in membership as users looked for other places to obtain their free music and other types of files. Files also fly around the Internet illegally through services such as AIM where friends exchange files, over local networks and members of various groups post files to servers where they can be exchanged. The Altavista search engine ([altavista.com/audio](http://altavista.com/audio)) does an excellent job finding arcane music files that are available on websites all over the Internet. A search for “muppets” turned up 197 songs that are over a minute in length and another 200 that are sound clips. This just shows how widely available pirated music is on the Internet and how easy it is to find if you know where to look, even if you choose not to use a P2P program or other source that most people would instantly mark as illegal. The Internet facilitates file-sharing, its job is to exchange information, but there is little judgment at the protocol level as to the legality of the files being

---

<sup>102</sup> A&M Records, Inc. v. Napster, Inc., 2001 U.S. Dist. LEXIS 2186 (N.D. Cal. Mar. 5, 2001).



shared.

#### 4.4 Privacy Protection in Policy

Hackers are one enemy of privacy. Everyone wants protection, yet with all the databases of information being compiled and then compromised, privacy seems to be more and more elusive. The US government is beginning to attempt to regulate Internet privacy through acts such as the Child Protection Act and regulations such as HIPAA. But while these policies will give some malicious information-gathering hackers pause, they simply show the public's growing concern over privacy of digital data and the legislator's reaction to these issues.

Children's privacy is protected under federal law with the Children's Online Privacy Protection Act of 1998, which prohibits websites from collecting personal information from children under the age of 13 without parental consent.<sup>103</sup> The intent of this was that parents were supposed to have a better idea what their children were doing on the net and be comfortable that their children were not being asked to supply any information that could lead to them getting in trouble. Clever kids simply learned to change their birth year and easily circumvent protections, but the sites were then protected as they did not know they were conducting business with a minor.

Medical records, which can contain very private information, are also protected by the regulations of the Health Insurance Portability and Accountability Act (HIPAA), a part of the department of Health and Human Services. These regulations pertain to privacy rights of medical documents and what patients can expect from their doctors concerning their personal information.<sup>104</sup> This includes basic security so a patient's records are only seen by people authorized to view the records ensuring the patient's right of privacy in their medical files. It also

---

<sup>103</sup> Children's Online Privacy Protection Act of 1998. <http://www.cdt.org/legislation/105th/privacy/coppa.html>  
Accessed 10.17.05.

<sup>104</sup> <http://www.hhs.gov/ocr/hipaa/>



guards against the misuse of patient records and protects their uses by healthcare providers, insurance and the health plans that may need to view or use the records.<sup>105</sup> Privacy of records which are not directly controlled by the patient is important, since it helps guarantee that those who take responsibility for the records will take efforts to keep them confidential.

The US Code contains some laws directly concerning hacking, specifically “Fraud and Related Activity in Connection with Computers” (18 USC 1030) which contains the legal definition of computer fraud being “having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure” for national defense, financial institutions, medical records and any computer involved in interstate commerce.<sup>106</sup> This law defines illegal hacking as *unauthorized access of a protected computer*.

The right to privacy is a hotly debated topic in all spheres of life, but when it comes to digital information, compromising that information is so easy that legislation only serves as guidelines for those who would obey and offers punishment for those who choose to disregard the rules. Policy is important because it gives us the right to persecute criminals, but it does not act well as a mode of prevention to those who will not be deterred by the law. It does define for security purposes what the law will prosecute and where extra effort should be instituted in order to avoid legal issues.

#### **4.5 Network Security**

One very important way that data needs to be protected from hackers is to be on the most secure network possible. The harder a network is to hack, the less likely it will be exploited by

---

<sup>105</sup> “GENERAL OVERVIEW OF STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION” <http://www.hhs.gov/ocr/hipaa/guidelines/overview.pdf>

<sup>106</sup> 18 USC 1030 - Fraud and Related Activity in Connection with Computers (a)(1) and (a)(2)(C).



script kiddies and the more likely it is that the network administrator can stop the malicious hacker before he does too much damage. And the more secure the network, the better and more determined the hacker must be to succeed.

Firewalls are only part of a solution. But they are an *important* part. The "thought of putting a web server (or any computer for that matter) on the Internet without installing a firewall in front of or on it has been considered suicidal."<sup>107</sup> A well-configured firewall can be an excellent defense against all but the most skilled hackers. But not all firewalls are well configured. Users allow them to develop holes for applications and do not go back later and remove those holes, leaving open access for hackers. Nor do they come out of the box correctly configured for maximum protection from hackers. Network administrators must make sure the firewall is properly configured.

Make no mistake, a well-designed, -configured, and -maintained firewall is nearly impenetrable. Most skilled attackers know this. They will simply work around the firewall by exploiting trust relationships and weakest-link security vulnerabilities, or they will avoid it entirely by attacking through a VPN or dial-up account.<sup>108</sup>

A firewall that is not so well-maintained can be broken and attackers will certainly try this method first. Certain ports can be left open for applications to use and a port-scan will quickly reveal these vulnerabilities.<sup>109</sup> Other firewalls allow remote login for telnet, Web and localhost and can lead to the network being compromised when a hacker gains access to various computers connected to the network.<sup>110</sup> Since these firewalls are configured to allow some access, they have the potential to let hackers in as well. Security is often compromised for usability.

---

<sup>107</sup> McClure pp 464.

<sup>108</sup> McClure pp 464.

<sup>109</sup> McClure pp 470.

<sup>110</sup> McClure pp 484.



But firewalls are not the only protection for networks. There are also hardware solutions to the network security issue. One emerging tech toy is Layer 7 Switches (Layer 7 is the top layer, the application layer in the OSI networking model; it is the layer most users interact with) which provide increased security. Routers can be setup with Access Control Lists (ACLs) which allows the router to record and identify and manage traffic.<sup>111</sup> Hardware and software protection work together to create a secure network environment. Each method affords protection, but these hardware methods tend to be expensive.

Wireless networks can be very insecure. Anyone can walk onto Sweet Briar's campus with a wireless card in their computer and access the LAN through the wireless network. The better the antenna you have, the further away you can pick up the wireless network.<sup>112</sup> Many hackers, looking for easy access to wireless networks use programs such as NetStumbler,<sup>113</sup> which allow the hacker to locate wireless networks in a geographic region. Cities such as Chicago have hundreds of unprotected wireless networks that users can stroll down the street and connect to.<sup>114</sup> People often do not think to secure their wireless networks since putting up similar security precautions is not necessary on a normal network. Wireless networks will often have no encryption, so data transferred across them can be accessed by anyone and no login requirements will be stipulated so anyone can log into unprotected networks.

The easiest way to protect against this is to set up your wireless network with encryption and MAC access control.<sup>115</sup> Each Ethernet connection on a computer has a unique MAC address that is associated with it which is not dynamic like an IP address and so never changes and can

---

<sup>111</sup> Davis, David. "Cisco IOS Access Lists: 10 Things you should know." June 16, 2005  
<<http://techrepublic.com.com/5102-1035-5731134.html>> Accessed 10.26.05

<sup>112</sup> Davis pp 411.

<sup>113</sup> Davis pp 418.

<sup>114</sup> Davis pp 424.

<sup>115</sup> Davis pp 444.



be used to accurately identify the specific computer. Wireless routers can be configured with access lists that only allow certain MAC addresses to log onto the wireless router, preventing unwanted intrusion.

Network security is an ever changing field where keeping up with the latest technology requires constant study. Network administrators must remain vigilant in an effort to keep the networks they are responsible for as secure as possible. Yet on top of prosecuting hackers and virus writers for breaches in security, some legal experts are now suggesting that network administrators should be held responsible.<sup>116</sup> While it is true that there are certainly cases of negligence on the part of the network administrators, it seems unnecessary to go after them when a foreign hacker is inaccessible to prosecutors or because they are simply a “better target for a lawsuit.”<sup>117</sup> Just because a guard dog fails to keep out trespassers does not mean one would sue the guard dog. Similarly, would it not make sense to go after the real criminal, the hacker? A network administrator who does his best to protect his network can still be outsmarted by a clever hacker. While there may be some fault on the part of the network administrator, it is the hacker who has committed the crime and so it is the hacker who should be tried. Prosecutors should not go after network administrators simply because the hackers cannot be found or tried.

Even the best network administrator is not completely able to protect his network. Users send information out to the Internet and receive it from others at a rate which would be impossible to fully control. So other forms of protection have sprung up to keep information safe.

#### **4.6 Information Security**

---

<sup>116</sup> Johnson, Vincent R. “Cybersecurity, Identity Theft, and the Limits of Tort Liability.” *South Carolina Law Review*. Vol 57, No 5. Winter 2005. Pp 255.

<sup>117</sup> Johnson pp 256.



In order to facilitate sharing of confidential information, various different encryption standards have been developed. As computers get faster and more efficient at processing data, they also get better at breaking the encryption of the various algorithms and so new methods with longer and more complicated keys have to be developed in order to keep the information secure. Various different methods of authentication are developed so that the receiving party can be sure the information they are getting has not been tampered with along the way. All of these methods propose to defeat hackers trying to intercept information by both the complexity of the keys and the various authentication steps that have to be completed before useful data is exchanged. Some protocols such as FTP do not use encryption so they are not secure ways to transfer data. Other protocols require more overhead due to the encryption but provide good protection for data.

Secure Socket Layer (SSL) is a popular encryption method in e-commerce used when buyers are sending sensitive financial data from their computer's web browsers to online merchants.<sup>118</sup> SSL requires that the sending and receiving computers synchronize the exchange of secret keys used to encrypt data. When using SSL, a small padlock appears on the bottom of the browser and a pop-up notice appears telling the user it is secure content (unless this feature has been disabled, which is common). All this allows for a relatively secure exchange of information that, even if intercepted, is encrypted and so protected from packet-snooping hackers.

Pretty good privacy (PGP) is another example of an individual and commonly used encryption standard which allows users to create their own private and public keys and then share encrypted documents.<sup>119</sup> PGP is now available from PGP Corporation. An individual

---

<sup>118</sup> Mel pp 215.

<sup>119</sup> Mel pp 193.



license costs \$99 and allows for a lifetime of file encryption and sharing.<sup>120</sup> It can also be found distributed for free on the net though these copies do not include the support.<sup>121</sup>

While PGP and SSL are two of the more common encryption methods that can be used to protect data during transit, there are many other encryption methods which use various different kinds of security to help users protect sensitive data. VPNs (Virtual Private Networks) used by businesses to access the company network from home or while traveling uses Internet Protocol Security (IPsec) which encrypts all data flowing to and from the computer.<sup>122</sup> Other ways to protect computers include Smart Cards, credit card sized objects that slide into the side of your computer and contain cryptographic keys that the computer reads to allow the user to log on and access data, programs and protocols stored on the computer. Once the smart card has been installed on the computer, the computer will not load without the card inserted inside.<sup>123</sup> These access keys, both the physical ones such as Smart Cards and the digital public and private keys, can be stolen and, once stolen, allow access to encrypted data. They also allow the hacker to use the keys to encrypt data that can then masquerade as being from the victim and so cause further damage to people who trust the victim.

Protecting these encryption keys comes down to the human element of security and many hackers are good at exploiting people and getting them to spill confidential information. Social engineering is one easy way for hackers to gain a critical piece of knowledge in order to corrupt a system. "People have a tendency to comply when the person making a request has been able to establish himself as likable, or as having similar interests, beliefs, and attitudes as the victim."<sup>124</sup> Hackers can play the role of the helpful technician, the friendly contractor, the confused

---

<sup>120</sup> <http://www.ppp.com/> Accessed 10.23.05.

<sup>121</sup> <http://www.pgpi.org/products/pgp/versions/freeware/> Accessed 10.23.05.

<sup>122</sup> Mel pp 230.

<sup>123</sup> Mel pp 259.

<sup>124</sup> Mitnick pp 247.



employee from another department and get people to spill information they would otherwise never speak of. So, even the best encryption can be compromised by users when they reveal sensitive information without double-checking who they are speaking to.

Individual users can also take steps to ensure the safety and security of their home computers when not connected to a larger network. Anti-virus programs which constantly watch for invasive material as well as desktop firewalls are an excellent start, though not a complete solution. Further programs that scan for ad-ware and spyware and block the pop-ups that often carry such annoyances can be used to further protect the computer. But at the individual user level, it is harder to ensure security. One can tell users what they should do, but as they will run the wide range from technically literate to barely able to power on their computer, these warnings may well be lost. The media's attention with hacking and having basic programs to protect computers could be good in this case as it encourages user awareness and at least compels home users to attempt some form of security. But in reality, while it is unlikely that a single, highly skilled hacker will target a home computer, the lack of good protection still leaves the individual computer vulnerable to threats from the trolling script kiddies and the damage done by viruses.

Again, the best way of protecting against hackers is awareness. Knowing what information is confidential and requiring users to provide some authentication before sharing it can go a long way towards protecting private data. Diligent use of encryption and careful protection of helps assure data confidentiality and integrity.

#### **4.7 Upcoming Changes**

Network security is rapidly evolving and as hacking is a huge problem; technology is evolving that addresses the issues people have raised about security. New viruses and worms are



on the rise to defeat systems once considered secure. Each new protection spawns new changes in hacking methods, just as each new virus forces security innovation to make technology safer. It is hardly surprising that the platforms we are accustomed to now, XP and OSX are undergoing these changes: XP to be replaced and OSX becoming a target for virus writers.

Microsoft's newest version of Windows, called Vista (initially called Longhorn), due out early next year, is said to have some interesting security settings. It features a new encryption technique called "BitLocker Drive Encryption which can be linked to a chip called TPM (Trusted Platform Module) in the computer's motherboard."<sup>125</sup> It also features InfoCards which are designed to help identify a user without releasing more information than is necessary. The overall goal is to create an operating system that is secure and reliable, addressing many security issues and adding new protections to user data. There are still disagreements among experts, though, as to whether these new methods are the correct answers to the security problems people are facing.

Harvard professor Lawrence Lessig is a voice in favor of Microsoft's new security measures. Instead of relying on a "hodgepodge of security measures" as we do now, he argues, Microsoft's new layer of protection will allow for a universal protocol that helps users both identify themselves as well as protect their identities.<sup>126</sup> Instead of being a software package like Passport was, InfoCards are a protocol, which will allow anyone to develop security with them. Lessig sees this as another case of an open source protocol innovating web security practices and saving users from malicious hackers.

Macintosh viruses – they do exist. For a long time, Apple users have gotten away with security through obscurity, Mac simply did not have enough of the market for virus writers, out

---

<sup>125</sup> Stone-Lee, Ollie. "UK Holds Microsoft Security Talks." *BBC News Online UK*. Posted February 16, 2006. Accessed February 22, 2006. <[http://news.bbc.co.uk/2/hi/uk\\_news/politics/4713018.stm](http://news.bbc.co.uk/2/hi/uk_news/politics/4713018.stm)>

<sup>126</sup> Lessig pp 98.



to create huge amounts of damage, to pay much attention to those small white boxes. “Today we received two more samples of Mac OS X malware,” starts a post on the F-Secure weblog.<sup>127</sup> Scrolling down the page are previous reports of new viruses targeting Apple systems and a clever graphic of the Mac logo with a band aid over it. So not only do viruses (worms in this case) now exist, they are starting to multiply. The new samples referred to were variations on another worm. Now that the Mac is using an Intel chip, imagine how much faster these viruses will come. Mac users are going to start waking up and realize that they need antivirus, and they are going to need it soon.

#### 4.8 Combining Approaches

Government and security both look at the problems hackers pose to information security and use their different tools to propose solutions to the problem. Government tries to legislate to cover all possible crimes while not restricting all communications. Network security faces the same problem, but addresses it from the other end: how to keep their networks as secure as possible without compromising usability. Security also tries to develop authentication methods which allow for fraud detection to prevent further fraud from occurring.

Both groups are fighting the same issues: security breaches and the frauds caused when these breaches happen. Network security is designed to prevent intrusion. Government provides the means to prosecute the crimes after they are committed. Both groups work together to create a system of protection and offense. Laws can regulate the code that controls networks to some extent and the possibilities of code can dictate laws. But each group tackles the problem from a different angle.

---

<sup>127</sup> Jarno. “Mac OSX Malware.” *F-Secure: News from the Lab*. Posted 2/21/06. Accessed 2/23/06. <<http://www.f-secure.com/weblog/archives/archive-022006.html#00000819>>



Network security is bent on keeping hackers out, making the network secure and preventing problems. Network administrators employ various methods of security such as encryption, firewalls and passwords to prevent intrusion while still allowing users all the access they require to be productive. They must also be vigilant to new developments, plugging new holes, exploring new security options, extracting viruses from their networks before they are allowed to develop and keeping hackers out. These network administrators are interested in legislation mainly so far as it concerns who they can keep out and what a hacker must do before he can be prosecuted. They may then gather the information needed to prosecute the hacker, but the actual prosecution is left to the government.

The government, on the other hand, looks at the problem from a different angle, not worrying about keeping the hackers out so much as dealing with the crimes they commit in hacking and after they have gained access. It provides the legislative backing required for network administrators to back their security up with the force of law. As the technology changes and develops, legislators are forced to revisit and revamp older laws to better fit the new problems and anticipate those still to come. The government often approaches technology as something to be tamed, the wilds of the Internet that need to be regulated. Some governments, such as China, do this by imposing nation-wide restrictions on information flowing in and out of the country. Others, such as the US, try to accomplish regulation by saying what it is illegal to use the Internet to do (e.g. fraud and child pornography). But the government's choices dictate how free network administrators are to make their own choices about what rules will govern their networks.

It would be difficult for one to operate successfully without the other. Without some form of government regulation, crimes such as hacking and fraud would not be clearly defined and



network administrators would have no place to start developing their own security rules. But a less restrictive system such as the US's does allow the network administrator to make choices about how much the network will be restricted, how much privacy is allowed and how carefully he protects data on the network. Network security provides government with an idea of what sorts of fraud are becoming common and what sorts of regulations the administrators are capable of installing on their networks. The government can regulate code, as can network administrators, but they still have a choice about how much they regulate and how they want to balance security with freedom for users.

#### **4.9 Summary / Conclusion**

If all electronic equipment is vulnerable to hacker attacks, then the best recourse is vigilance in updating and protecting critical information. This may mean physical security such as Smart Cards, locking a laptop to a desk or more sophisticated hardware or it could mean electronic security such as a firewalls, encryption and software updates. It also means making sure to connect to a secure and reliable network. A network can be secure and restrictive of its users or less secure but allowing more freedom.

Information can be encrypted, but the encryption keys still have to be protected. Digital encryption and public keys are good methods of protection, but are not perfect. And because they can be broken, researchers are working on developing new methods of security that are harder to break and more difficult to falsify. Information can be intercepted and replaced by less-reliable information; keys can be faked and stolen. Even the best encryption can grow outdated as faster machines come along to break older algorithms. Policy and security software can only take us so far in protecting ourselves from hackers. The rest is up to the user who needs to be aware and



vigilant of what is happening with their data and take steps to protect it so it doesn't fall into the wrong hands.



## Section 5 – Conclusion

### 5 – Conclusion

So, who are the hackers? This paper has discussed script kiddies, black- and white-hat hackers, virus writers, security specialists and researchers. But who is the hacker? Can we ever be sure or do we just need to get close enough to keep ourselves safe? We can line up the profile of a typical hacker, young, male, geeky, but that is also the profile of a great technician, a friendly network administrator or a great graphics designer. Hackers are not one type of person, they are many types. The good ones have an interest in security, knowing the insides of hacking so they can prevent it. The bad ones are sometimes interested in information, getting at it or destroying it and sometimes interested in reputation, proving they can accomplish a certain hack or enter a certain system. The media portrays them as bad, but it is their malicious actions that make them so, not their knowledge of computer security (or insecurity).

How much threat is really presented by hackers depends on the system to which you are connected and what sorts of information your computer stores. Script kiddies and crashed computers are mere annoyances compared to the damage an elite hacker can do when he compromises a network to access data or crash thousands of computers. To individual users, viruses are far more of a threat to a single system than an elite hacker. Even a system with lots of computers connected but not much valuable data is likely to be hacked only to be used as storage or as a further hop to somewhere than for the limited data that network may contain.

What hackers do varies as widely as the types of people who hack. Some try to figure out ways to defeat other hackers; others try to find ways to beat the system. The very definition of a hacker is someone who comes up with a new or clever way to do something and it is their innovation that causes their ability to access so much and spurs innovation designed to defeat



them. But with changes in technology come changes in hacking as clever hackers find ways around the security they are presented with.

Some systems, it is true, are excellently resilient to hacker attacks, whether through good hardware or excellent administration. But the hacker is often a disgruntled or recently fired employee with a good knowledge of the system and the credentials to get in. It is hard to target exactly who the hacker is, and so defense against hackers is defense against an unknown enemy.

Network security defends against hackers by trying to prevent their entry in the first place. Administrators make sure their network is secure against known and possible hacker attacks and are constantly on the lookout for new attacks or improvements that can make their networks more secure.

The government takes a different approach, restricting certain activities on the Internet and providing punishments for those who engage in them. From child pornography to fraud, the laws in the US are restrictive of things considered to be crimes but not outside of the range of misdeeds. Legislators and judges continuously look at laws and update definitions and crimes as technology changes to include more aspects of life.

This combined effort on the part of network security and the government results in a computer environment that is mostly secure against malicious hackers, making their goals harder to achieve, making it easier to catch them and finally giving the government something to accuse them of doing illegally.

Where government regulation lets off, network security starts. A network administrator can choose to have a very secure and highly regulated network or a freer but less secure network, depending on his personal tastes and the requirements of the network. It is always a fine line to walk, a choice between freedom of exchange and regulation of information.



The desire for instantaneous access to information – the desire to be able to retrieve information quickly across a network or from the Internet brings with it the danger of security breaches. To believe otherwise is to be utopian. If people want this information infrastructure, then they must get comfortable with a redefined sense of privacy. To be completely secure, one would have to make no transactions that pass personal information into an electronic format – something which in today's society is a near impossibility. Otherwise, one must assume that data, even well-protected and encrypted data, will never be perfectly secure.









